This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0023129
Application Number

출 원 년 월 일 : 2003년 04월 11일
Date of Application APR 11, 2003

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2004 년 04 월 19 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】 특허출원서
【권리구분】 특허
【수신처】 특허청장
【참조번호】 0003
【제출일자】 2003.04.11
【국제특허분류】 H04M
【발명의 명칭】 이동통신 시스템에서 암호화를 이용한 방송 서비스 방법
【발명의 영문명칭】 BROADCASTING SERVICE METHOD USING ENCRYPTION IN MOBILE TELECOMMUNICATION SYSTEM
【출원인】
【명칭】 삼성전자 주식회사
【출원인코드】 1-1998-104271-3
【대리인】
【성명】 이건주
【대리인코드】 9-1998-000339-8
【포괄위임등록번호】 2003-001449-1
【발명자】
【성명의 국문표기】 정정수
【성명의 영문표기】 JUNG,Jung Soo
【주민등록번호】 770607-1690714
【우편번호】 143-191
【주소】 서울특별시 광진구 자양1동 617-41 1층 2호
【국적】 KR
【발명자】
【성명의 국문표기】 김대균
【성명의 영문표기】 KIM,Dae Gyun
【주민등록번호】 681003-1690413
【우편번호】 463-773
【주소】 경기도 성남시 분당구 서현동 시범우성아파트 228동 1703호
【국적】 KR
【발명자】
【성명의 국문표기】 배범식
【성명의 영문표기】 BAE,Beom Sik

【주민등록번호】 710821-1009411
【우편번호】 442-809
【주소】 경기도 수원시 팔달구 영통동 955-1 황골마을 주공아파트 121동 1102 호
【국적】 KR

【발명자】
【성명의 국문표기】 송준혁
【성명의 영문표기】 SONG,Jun Hyuk
【주민등록번호】 710321-1046916
【우편번호】 431-070
【주소】 경기도 안양시 동안구 평촌동 19-1블럭 꿈마을 아파트 203동 402호
【국적】 KR

【발명자】
【성명의 국문표기】 장용
【성명의 영문표기】 CHANG,Yong
【주민등록번호】 700318-1655313
【우편번호】 463-780
【주소】 경기도 성남시 분당구 수내동(푸른마을) 신성아파트 403동 801호
【국적】 KR

【발명자】
【성명의 국문표기】 임내현
【성명의 영문표기】 LIM,Nae Hyun
【주민등록번호】 730813-1011631
【우편번호】 135-280
【주소】 서울특별시 강남구 대치동 960-15
【국적】 KR

【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 이건주 (인)

【수수료】
【기본출원료】 20 면 29,000 원
【가산출원료】 39 면 39,000 원

【우선권주장료】	0	건	0 원
【심사청구료】	0	항	0 원
【합계】	68,000	원	

【요약서】

【요약】

본 발명은 이동통신 시스템에서 무선채널을 통해 이동 단말에게 방송서비스를 제공하기 위한 방법에 대한 것이다. 기지국은 단말로부터 수신한 등록 메시지에 포함된 등록 식별자에 따라 상기 단말이 암호화 키를 요구하는지의 여부를 판단하고, 요구하는 것으로 판단된 경우에만 현재 유효한 암호화 키를 전송한다. 이때 기지국은 상기 등록 메시지가 현재 유효한 암호화 키의 유효시간이 종료되기 이전 미리 정해지는 유도시간 이내에 수신된 경우에 현재 유효한 암호화 키와 함께 다음에 사용될 암호화 키를 전송한다. 단말은 현재 암호화 키를 가지고 방송 서비스 도중 상기 암호화 키에 대응하는 등록 식별자를 포함하는 등록 메시지를 기지국으로 전송하고, 그에 대한 응답으로 기지국으로부터 현재 유효한 암호화 키 및 다음에 사용될 암호화 키를 수신한다. 그리고 현재 암호화 키의 유효시간이 종료되면 상기 다음 암호화 키를 사용하여 연속적으로 방송 서비스를 수신한다. 이러한 본 발명은 등록 메시지에 응답하여 암호화 키를 제공하는 방송 서비스 시스템에서 불필요한 메시지의 전송과 처리를 제거하여 시스템 부담을 감소시킬 수 있다.

【대표도】

도 9

【색인어】

Broadcast Multicast Service, PDSN, PCF, AAA, Encryption key, Registration

【명세서】

【발명의 명칭】

이동통신 시스템에서 암호화를 이용한 방송 서비스 방법{BROADCASTING SERVICE METHOD USING ENCRYPTION IN MOBILE TELECOMMUNICATION SYSTEM}

【도면의 간단한 설명】

도 1은 전형적인 방송서비스 시스템의 전체 구성을 나타낸 도면.

도 2는 상기 도 1에 나타낸 방송 서비스 시스템의 프로토콜 스택을 나타낸 도면.

도 3은 전형적인 단말과 기지국간의 방송형 서비스 절차를 나타낸 메시지 흐름도.

도 4는 방송 서비스를 위해 사용되는 위치등록 메시지의 포맷.

도 5는 전형적인 방송서비스 시스템을 통한 방송형 서비스. 절차를 나타낸 메시지 흐름도.

도 6은 전형적인 방송서비스 시스템에서 기지국에 의해 등록을 수행하는 동작을 나타낸 메시지 흐름도.

도 7은 전형적인 방송 서비스 시스템에서 패킷 데이터 서비스 노드(PDSN)에 의해 등록을 수행하는 동작을 나타낸 메시지 흐름도.

도 8은 본 발명의 일 실시예에 따라 암호화 키의 관련 정보를 포함하는 등록 메시지의 포맷.

도 9는 본 발명에 따라 암호화 키의 해시 값을 사용하여 등록을 수행하는 방송 서비스 동작을 나타낸 메시지 흐름도.

도 10은 본 발명의 변형된 실시예에 따라 암호화 키의 시퀀스 번호를 포함하는 등록 메시지의 포맷.

도 11은 본 발명의 다른 변형된 실시예에 따라 암호화 키 요구 비트를 포함하는 등록 메시지의 포맷.

도 12는 본 발명에 따라 등록 식별자를 사용하는 단말의 등록 동작을 나타낸 흐름도.

도 13은 본 발명에 따라 등록 식별자를 사용하는 기지국의 등록 동작을 나타낸 흐름도.

도 14는 본 발명에 따라 유도시간을 사용하는 방송 서비스 절차를 나타낸 메시지 흐름도.

도 15는 본 발명에 따라 현재 암호화 키 및 다음 암호화 키를 포함하는 데이터 버스트 메시지의 포맷.

도 16은 본 발명에 따라 현재 암호화 키 및 다음 암호화 키를 포함하는 암호화 정보 메시지의 포맷.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<17> 본 발명은 이동통신 시스템에 관한 것으로서, 특히 무선채널을 통해 이동 단말에게 방송 서비스를 제공하기 위한 방법에 대한 것이다.

<18> 미래의 통신환경은 유선과 무선의 영역구분이나 지역이나 국가의 구분을 초월한 만큼 급변하고 있다. 특히, IMT-2000(International Mobile Telecommunication 2000) 등과 같은 미래

통신환경은 영상과 음성은 물론 사용자가 필요로 하는 다양한 정보를 실시간으로 그리고 종합적으로 제공하는 환경으로 구축되는 추세이다. 이동통신 시스템의 발달은 셀룰러폰(cellular phone)이나 PCS(Personal Communication System) 등의 이동 단말(Mobile Station: MS)에서 단순히 음성통신만을 수행하던 차원에서 벗어나 문자 정보의 전송은 물론, 방송서비스를 시청할 수 있는 정도까지 도달해 있다.

<19> 전형적인 무선통신 시스템에서 방송 데이터의 전송은 단일 전송(Unicast)에 의해 이루어져왔다. 동시에 복수의 단말들에게 동일한 데이터를 전송하여야 하는 방송 서비스의 특성상, 단일 전송은 시스템과 무선 구간에서 자원의 낭비를 가지고 오며 시스템의 부하를 가중시키는 원인이 된다. 따라서 시스템 자원을 절약하면서 고품질의 방송 서비스를 제공하기 위한 다양한 기술이 연구되고 있다.

<20> 현재 3GPP2(3rd Generation Partnership Project 2)에서는 이동통신 시스템에서 방송서비스를 위해 다양한 서비스 매체 및 효율적인 자원이용을 고려하고 있다. 이러한 방송서비스는 이동 단말로부터의 역방향 반환정보 없이 고속의 순방향 데이터를 단방향 송신함으로써 이루어진다. 이는 개념상 일반 텔레비전 방송 서비스와 유사하다고 할 수 있다.

<21> 비-상업적 서비스 차원에서 방송 서비스를 제공한다면 불특정 다수의 단말들이 기지국으로부터 단말 방향으로의 하향 트래픽 채널을 액세스할 수 있도록 하면 된다. 반면에 경제적 이익을 목적으로 하는 상업적 텔레비전 방송 서비스를 사용자들에게 제공하고자 한다면, 시스템은 인증된 단말기들만이 방송을 수신하고 인증되지 않은 단말기들은 방송을 수신할 수 없도록 하여야 하며, 인증된 단말기들이 방송 서비스를 이용한 시간을 측정하여 정확한 요금을 부과하여야 한다. 그런데 종래의 이동통신 시스템에서는 단말이 방송 서비스를 이용하는 시점을 제어

할 수 없기 때문에 불법 단말의 방송 서비스 액세스를 제한할 수 없었으며 효율적인 과금이 불가능하였다는 문제점이 있었다.

【발명이 이루고자 하는 기술적 과제】

<22> 따라서 상기한 바와 같이 동작되는 종래 기술의 문제점을 해결하기 위하여 창안된 본 발명은 본 발명은 이동통신 시스템으로 위치등록을 수행하는 이동 단말들에게 방송 서비스를 위해 소정의 유효시간을 가지는 암호화 키를 제공한다.

<23> 본 발명은 이동통신 시스템에서 방송 서비스를 위해 이동 단말들로부터 전송되는 위치등록 메시지들에 의한 역방향 오버헤드를 감소시키는 방법을 제공한다.

<24> 본 발명은 이동통신 시스템에서 이동 단말들의 위치등록에 의한 시스템 오버헤드를 감소시키는 방법을 제공한다.

<25> 본 발명의 일 실시예는, 무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 상기 단말에서 방송 서비스를 제공받는 방법에 있어서,

<26> 상기 이동통신 시스템에 방송 서비스의 지속적인 제공을 요청하기 위해 기 수신한 암호화 키를 식별하는 등록 식별자를 포함하는 등록 메시지를 생성하여 상기 기지국으로 전송하는 과정과,

<27> 상기 등록 메시지에 응답하여 방송 서비스를 위해 암호화 키를 포함하는 암호화 정보 메시지를 수신하는 과정과,

<28> 방송 서비스 채널을 통해 상기 기지국으로부터 수신한 방송 데이터를 복호화하기 위해 상기 암호화 정보 메시지에 포함된 암호화 키를 저장하고, 상기 암호화 키에 대응하여 상기 등록 식별자를 갱신하는 과정을 포함하는 것을 특징으로 한다.

<29> 본 발명의 다른 실시예는, 무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 상기 기지국에 의해 상기 단말에게 방송 서비스를 제공하는 방법에 있어서,

<30> 상기 단말로부터 상기 이동통신 시스템에 방송 서비스의 제공을 요청하기 위한 등록 메시지를 수신하는 과정과,

<31> 상기 등록 메시지에 따라 상기 단말로부터 암호화 키가 요구되는지를 판단하는 과정과,

<32> 상기 암호화 키가 요구되는 것으로 판단되면, 방송 서비스를 위한 암호화 키를 포함하는 암호화 정보 메시지를 상기 단말로 전송하는 과정을 포함하는 것을 특징으로 한다.

<33> 본 발명의 또 다른 실시예는, 무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 상기 단말에서 방송 서비스를 제공받는 방법에 있어서,

<34> 소정 유효시간을 가지는 암호화 키를 가지고 방송 서비스를 진행하는 도중 미리 정해지는 위치등록 조건이 만족될 때 상기 이동통신 시스템에 방송 서비스의 계속적인 제공을 요청하기 위한 등록 메시지를 생성하여 상기 기지국으로 전송하는 과정과,

<35> 상기 등록 메시지에 응답하여 방송 서비스를 위해 다음 암호화 키와 상기 다음 암호화 키의 유효시간을 포함하는 암호화 정보 메시지를 수신하는 과정과,

<36> 현재 암호화 키를 가지고 방송 서비스를 수신하면서 상기 현재 암호화 키의 유효시간이 종료되었는지를 판단하는 과정과,

<37> 상기 현재 암호화 키의 유효시간이 종료되었으면 상기 다음 암호화 키를 가지고 연속적으로 방송 서비스를 수신하는 과정을 포함하는 것을 특징으로 한다.

<38> 본 발명의 또 다른 실시예는, 무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 상기 기지국에 의해 상기 단말에게 방송 서비스를 제공하는 방법에 있어서,

<39> 소정 유효시간을 가지는 암호화 키를 가지고 방송 서비스를 진행하는 도중, 상기 단말로부터 상기 이동통신 시스템에 방송 서비스의 계속적인 제공을 요청하기 위한 등록 메시지를 수신하는 과정과,

<40> 상기 등록 메시지가 상기 암호화 키의 유효시간이 종료되기 이전 미리 정해진 유도시간 내에 수신된 것으로 판단되면, 방송 서비스를 위해 다음 암호화 키와 상기 다음 암호화 키의 유효시간을 포함하는 암호화 정보 메시지를 상기 단말로 전송하는 과정을 포함하는 것을 특징으로 한다.

【발명의 구성 및 작용】

<41> 하기에서 본 발명을 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용

자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

<42> 후술되는 본 발명은 이동통신 시스템에서 방송 서비스(Broadcast Service: BCS)를 제공함에 있어서, 위치 등록을 수행하는 이동 단말들에게 방송 서비스를 위해 소정의 유효시간을 가지는 암호화 키(Encryption key)를 제공하는 것이다. 특히 본 발명은 이동 단말들의 위치 등록으로 인한 시스템 오버헤드 및 무선 구간의 역방향 오버헤드를 감소시키기 위해 등록 식별자와 유도시간(skew time)을 사용한다.

<43> 이하 본 발명의 실시예를 설명하기에 앞서 전형적인 방송 서비스의 동작을 설명하기로 한다.

<44> 도 1은 전형적인 방송서비스 시스템의 전체 구성을 나타낸 것이다.

<45> 상기 도 1을 참조하면, 방송서버(Broadcasting Service Server or Contents Server: CS) 14는 방송서비스를 위한 영상(Video) 및/또는 음향(Sound)을 포함하는 방송 데이터를 패킷 데이터 서비스 노드들(Packet Data Service Node: PDSN) 13을 통해 기지국들(Base Station: BS) 11a,11b로 전달된다. 상기 방송서버 14가 인터넷 등의 패킷 통신 네트워크를 통해 상기 패킷 데이터 서비스 노드 13에 연결되는 경우, 상기 방송 데이터는 압축된 인터넷 프로토콜(Internet Protocol: IP) 패킷의 형태로 생성된다.

<46> 상기 패킷 데이터 서비스 노드 13은 인증 및 과금(Authentification, Authorization and Accounting) 서버 15로부터 패킷 통신의 인증을 위한 사용자 프로파일 정보를 제공받으며 방송 서비스를 위한 과금 정보를 생성하여 상기 인증 및 과금 서버 15로 제공한다. 상기 기지

국들 11a,11b는 셀룰러 이동통신 기술분야에서 잘 알려진 기지국 송수신기들(Base Transceiver Subsystems: BTSs) 11a-1, 11a-2, 11b-1,11b-2와 기지국 제어기들(Base Station Controllers: BSCs) 11a-3, 11b-3을 포함하는 것으로서 패킷 데이터의 통신을 위한 패킷 제어기들(Packet Control Function blocks: PCF) 12a,12b를 통해 상기 패킷 데이터 서비스 노드 13에 연결된다.

<47> 일 예로서, 상기 방송서버 14에 의하여 생성된 방송 데이터를 기지국들 11a,11b로 전달하기 위해서는 IP 멀티캐스트(Multicast)가 이용된다. 상기 기지국들 11a,11b는 상기 방송서버 14로부터 IP 멀티캐스트 데이터를 제공받는 멀티캐스트 그룹(Multicast Group)을 형성한다. 상기 멀티캐스트 그룹의 소속정보(Membership Information)는 상기 기지국들 11a,11b 각각에 연결되는 멀티캐스트 라우터(Multicast Router: MR)(도시하지 않음)에 의하여 유지된다.

<48> 상기 방송 서버 14에서 생성된 IP 멀티캐스트 데이터는 멀티캐스트 그룹을 형성하는 복수의 기지국들 11a,11b에게 브로드캐스팅되고, 상기 기지국들 11a,11b는 상기 IP 멀티캐스트 데이터를 무선 주파수(Radio Frequency: RF) 신호의 형태로 변환하여 해당 서비스영역에서 송출한다.

<49> 도 2는 상기 도 1에 나타낸 방송 서비스 시스템의 프로토콜 스택을 나타낸 것으로서, 여기서 언급하는 계층(Layer)이란 해당 프로토콜에 따른 동작을 수행하는 소프트웨어 블럭 또는 하드웨어를 의미한다.

<50> 상기 도 2를 참조하면, 인터넷 프로토콜(Internet Protocol)을 통해 방송 서비스를 제공받는 단말(MS)은 제1 계층(Layer 1: L1)인 물리계층(Physical Layer)과, MAC(Media Access Control) 계층과, 제2 계층(L2)인 링크(Link) 계층/PPP(Point to Point Protocol) 계층과 제3 계층(L3)인 IP(Internet Protocol) 계층을 기반으로 하고, 사용자 데이터 프로토콜(User Datagram Protocol: UDP)과 실시간 전송 프로토콜(Real-Time Protocol: RTP) 등을 지원하는 운

송(Transport) 계층과, MPEG(Moving Picture Experts Group)-4 등을 지원하는 응용(Application) 계층을 더 포함하여 구성된다.

<51> 기지국/패킷 제어기(BS/PCF)는 단말과의 통신을 위한 물리계층과 링크 계층 및 패킷 데이터 서비스 노드(PSDN)와의 통신을 위한 제1 및 제2 계층으로 구성된다. 패킷 데이터 서비스 노드는 기지국/패킷 제어기와의 통신을 위한 제1, 제2 계층 및 PPP 계층과 패킷 데이터 네트워크와의 통신을 위한 제1 및 제2 계층을 기반으로 하고 IP 계층을 더 포함하여 구성된다. 방송 서버는 적어도 하나의 라우터로 이루어진 패킷 데이터 네트워크와의 통신을 위한 제1, 제2 계층 및 IP 계층을 기반으로 하고, 단말에게 제공할 방송 데이터를 생성하고 전송하기 위해 MPEG-4 등을 지원하는 응용 계층과 운송 계층을 더 포함하여 구성된다.

<52> 부가적으로 방송 서버와 단말간에 별도의 암호화를 사용하는 경우 방송 서버와 단말은 방송 데이터의 암호화(encryption) 및 복호화(decryption)를 위한 암호화(Encryption) 계층을 포함하나, 여기에서의 암호화 및 복호화를 위한 암호화 키는 방송 서비스의 초기화시에 방송 서비스 파라미터 메시지(Broadcast Service Parameter Message: BSPM) 등을 통하여 제공될 뿐 주기적으로 갱신되는 것이 아니므로 방송 서비스의 인증 및 과금에 적용될 수 없다. 따라서 본 명세서에서는 방송 서버와 단말간의 암호화에 대한 보다 상세한 설명을 생략할 것이다.

<53> 도 3은 전형적인 단말과 기지국간의 방송형 서비스 절차를 나타낸 메시지 흐름도이다.

<54> 상기 도 3에서, 전원이 인가되면 단말은 초기화(Initialization)를 수행한 후 방송형 서비스를 수신하기 위해서 자신이 동조되어 있는 주파수 대역(f_{HASH})을 통

해 기지국에서 공통 채널로 송신하는 방송서비스 파라미터 메시지(Broadcast Service Parameter Messages: BSPM)를 수신하여 방송형 서비스에 대한 세션 정보를 획득한다. 상기 BSPM은 방송 서비스를 위한 물리채널의 주파수 및 부호 정보와, 기지국에서 제공 가능한 방송 서비스들을 나타내는 BCS ID(Broadcast Service Identifier) 등의 방송 서비스 파라미터를 포함한다. 단말은 상기 방송 서비스 파라미터에 의해 논리적 방송 서비스 정보와 물리채널 사이의 매핑 여부를 확인하고, 해당 물리채널을 액세스한다.

<55> 단말은 BSPM에 포함된 n개의 방송 서비스들에 대한 BCS ID들, BCS1, BCS2, ... BCSn 중 원하는 방송 서비스의 BCS ID, 예를 들어 BCS2를 획득하고, 마찬가지로 상기 BSPM을 통해 알아낸 해당 서비스 주파수(f_{BCS2})로 전환한 후 상기 서비스 주파수에서 순방향 방송채널(Forward Broadcast Service Channel: F-BSCH)을 통해 방송 데이터를 수신한다. 단말 사용자가 방송 서비스를 종료하기를 원한다면 단말은 f_{BCS2}의 모니터링을 중지하고 원래의 주파수인 f_{HASH}로 되돌아간다. 음영으로 표시된 부분은 단말이 방송서비스를 받고 있는 시간구간을 나타낸다.

<56> 이동통신 시스템으로 제공되는 방송 데이터는 방송용 채널을 이용해 무선으로 방송된다. 이러한 방송 서비스에서 시스템 사용자 측면에서 중대하게 요구되는 특징은 인증되지 않은 단말 또는 불법적인 단말이 방송 데이터를 수신할 수 없도록 하는 것이다. 게다가 단말은 방송서비스 도중에도 음성 호 서비스를 위한 착신 요구, 즉 시스템에 의한 호출 신호를 받을 수 있어야 한다.

<57> 따라서 방송서비스 시스템에서는 방송 데이터 트래픽을 소정 유효시간 동안 해당하는 암호화 키를 가지고 복호가 가능하도록 암호화하여 전송하고, 방송 서비스 도중 주기적 또는 비주기적으로 위치등록을 수행하는 이동 단말들에게 방송 데이터 트래픽의 복호를 위한 암호화

키를 제공한다. 이는 방송 서비스를 제공받는 이동 단말들에게 위치등록을 수행하도록 강제함으로써, 불법적인 사용을 방지하고 착신 요구를 정상적으로 수신할 수 있도록 하기 위함이다.

<58> 위치등록은 시스템과 단말 사이에 미리 약속된 등록 메시지를 기지국으로 전송함으로써 이루어진다. 도 4는 본 발명에 따른 위치등록 메시지의 포맷을 나타낸 것이다. 상기 도 4를 참조하여 위치등록 메시지의 주요 필드들을 살펴보며, REG_TYPE 필드는 위치등록 이유를 나타내고, NUM_BCS_SESSION은 방송 서비스를 위해 연결된 세션 개수를 나타내고, 상기 세션 개수에 따라 방송 서비스를 위한 필드들이 이어진다. 방송 서비스를 위한 필드들로는, 요구되는 방송 서비스의 내용을 나타내는 BCS_ID 필드와 방송 서비스의 종료 여부를 나타내는 DE_REG_IND가 있다.

<59> 단말의 위치등록은 시간제 등록(Time Based Registration), 시스템의 호출 메시지에 의한 지시된 등록(Ordered Registration) 또는 암호화 키의 유효시간 종료 등의 소정 위치등록 조건이 만족될 때에 이루어지며, 시스템은 위치등록 메시지의 REG_TYPE 필드로서 단말이 위치등록을 수행하는 이유를 구별한다. 상기 REG_TYPE 필드의 값들을 간단히 설명하면, '0000'은 이동 단말이 미리 정해지는 위치등록 주기에 도달하였을 때, '0001'은 전원이 켜졌을 때, '0010'은 새로운 위치등록 영역(Registration Zone)으로 진입할 때, '0011'은 전원이 꺼질 때, '0100'은 파라미터가 변경되었을 때, '0101'은 시스템으로부터 위치등록이 지시되었을 때, '0110'은 기지국으로부터의 거리가 소정 단위로 변화할 때, '0111'은 새로운 사용자 영역으로 진입하였을 때 위치등록을 수행함을 의미한다. 또한 '1000'은 방송서비스를 개시하거나 유지하기 위한 위치등록을 의미한다.

<60> 도 5는 전형적인 방송서비스 시스템을 통한 방송형 서비스 절차를 나타낸 메시지 흐름도이다. 여기에서는 인증(authentication) 등 본 발명과 관계가 없는 일부 흐름을 생략하거나 간략하게 나타내었다.

<61> 상기 도 5를 참조하면, 단말은 방송 서비스를 시작하면서 과정(a)에서 데이터 서비스를 나타내는 서비스 옵션(Service Option: SO) 번호 33(SO 33)을 포함하는 발신 메시지(Origination Message: ORM)를 기지국으로 전송하여 과정(b)과 같이 트래픽 채널을 설정한 후, 과정(c)과 같이 패킷 데이터 서비스 노드(PDSN)와 PPP 연결을 설정한다. 단말은 과정(d)과 같이 상기 PPP 연결을 통해 얻은 DNS(Domain Name Systems) 서버의 주소 정보를 이용하여 상기 DNS 서버에 방송 서비스 제어기(BCMCS controller)의 IP 주소를 문의하고, 과정(e)과 같이 DNS 서버로부터 방송 서비스(BCS) 제어기의 IP 주소를 받는다.

<62> 그러면, 과정(f)에서 단말은 방송 서비스 제어기에게 사용자가 원하는 방송 서비스에 대한 정보를 요구하게 되며, 과정(g)에서 방송 서비스 제어기는 상기 단말에 대한 인증 처리 후 요구된 방송 서비스 관련 정보를 제공한다. 상기 정보에는 방송 데이터를 수신할 수 있는 공통 암호화 키(Broadcast Access Key: BAK) 정보, 상기 공통 암호화 키의 유효 시간, 멀티캐스트 IP 주소 및 포트 정보 등을 포함한다.

<63> 상기 방송 서비스 관련 정보를 수신한 단말은 과정(h)과 같이 오버헤드 채널을 통해 기지국으로부터 방송 서비스 파라미터 메시지(BSPM)를 수신하고, 기지국에서 지원 가능한 방송 서비스에 해당하는 트래픽 채널의 정보 등을 얻은 후, 과정(i)과 같이 기지국으로 방송 서비스를 요구하기 위한 등록 메시지를 전송하여 방송 서비스 수신을 시작한다. 만약 기지국에서 처음으로 방송 서비스가 요구되었다면, 기지국은 과정(j)과 같이 운반 설정(Bearer Setup) 절차를 수행한다. 요구된 방송 서비스를 위한 채널이 이미 설정되어 있는 경우에는 상기 과정(j)은

필요치 않다. 이후 과정(k)에서 단말은 해당 방송 서비스를 수신하며, BAK가 유효한 시간 동안 BSPM 메시지의 수신과 등록 메시지의 전송만으로 방송 서비스의 수신이 가능하다.

<64> 상기 도 5에 나타낸 방송형 서비스를 제공하는 시스템에서 사용하는 암호화 키 BAK는 방송형 서비스를 수신하는 모든 단말들에서 사용하는 공통 암호화 키이므로 사용자별 과금이 불가능하다. 따라서 하기의 도 6 및 도 7과 같이 단말의 등록에 의해 사용자별 인증이 가능한 방송형 서비스가 제안되었다.

<65> 도 6은 전형적인 방송서비스 시스템에서 기지국에 의해 단말의 등록을 수행하는 동작을 나타낸 메시지 흐름도이다. 여기에서 단말은 방송 서버로부터 방송 서버와 세션을 연결하기 위해 필요한 방송용 서비스 파라미터를 BSPM을 통해 이미 수신한 것으로 한다.

<66> 상기 도 6을 참조하면, 과정(a)에서 단말은 방송 서비스를 요구하기 위해 기지국으로 등록 메시지를 전송한다. 상기 등록 메시지의 포맷은 앞서 언급한 도 4에 나타낸 바와 같다. 상기 등록 메시지는 단말의 위치를 이동통신 시스템으로 등록함과 동시에 수신하고자 하는 방송 서비스의 종류를 기지국으로 전달하며, 또한 방송 서비스를 위한 암호화 키를 요구하기 위한 것이다. 단말의 위치는 상기 등록 메시지를 수신하여 시스템으로 전달하는 기지국의 식별자에 의하여 알려지며, 단말이 수신하고자 하는 방송 서비스의 종류는 상기 등록 메시지에 포함되는 BCS_ID 필드에 의해 알려진다.

<67> 과정(b)에서 기지국은 단말로부터 BCS_ID를 포함하는 등록 메시지를 최초로 수신하면, 단말로부터 방송 서비스가 요구된 것으로 판단하고 상기 BCS_ID에 해당하는 방송 서비스를 위해 현재 시점에서 공통 암호화 키(BAK)와는 다른 암호화 키(X key)를 생성하여 데이터 버스트 메시지(Data Burst Message: DBM) 또는 암호화 정보 메시지(Encryption Information Message: EIM)에 실어 페이징 채널(Paging Channel) 또는 순방향 공통 제어 채널(Forward Common

Control Channel: F-CCCH)을 통해 단말로 전송한다. 동시에 기지국은 상기 단말의 위치 정보를 교환기(도시하지 않음) 또는 AAA 서버로 전달하여 등록한다.

<68> 상기 데이터 버스트 메시지 또는 상기 암호화 정보 메시지는 상기 암호화 키 자체 또는 상기 암호화 키를 생성하는데 사용되는 생성 정보, 즉 시드(seed)와, 선택적으로 상기 암호화 키의 유효시간을 운반한다. 다른 경우 상기 암호화 키는 기지국이 아닌 별도의 개체에 의해서 생성되어 기지국으로 제공될 수 있다. 도 6에서 상기 암호화 키는 X로 표기되었으며 미리 정해지는 소정의 유효시간을 가진다.

<69> 과정(c)에서 단말은 상기 암호화 키를 성공적으로 수신하거나 또는 상기 시드를 수신하여 상기 암호화 키를 성공적으로 생성하면 기지국으로 긍정응답(Acknowledge: Ack) 메시지를 전송한다. 과정(d)에서 기지국은 단말로부터 Ack 메시지를 수신하면 상기 암호화 키가 성공적으로 수신된 것으로 판단하여, 현재의 시간으로 설정된 단말의 시간 스탬프(time stamp) 정보와 상기 BCS_ID를 IOS(Inter Operability Specification) 메시지에 실어 패킷 데이터 서비스 노드로 전송한다. 만일 단말로부터 암호화 키를 포함하는 데이터 버스트 메시지에 대한 응답이 수신되지 않으면 기지국은 단말로부터 응답이 수신될 때까지 미리 지정된 회수만큼 상기 암호화 키를 포함하는 데이터 버스트 메시지를 재전송한다.

<70> 과정 (e)에서 패킷 데이터 서비스 노드는 상기 IOS 메시지에 응답하여 단말기 별로 방송 서비스 접속 시간에 대한 정보, 즉 과금 정보를 과금 요구(Accounting Request) 메시지에 실어 AAA 서버로 전송한다. 그러면 과정(f)에서 AAA 서버는 상기 과금 정보를 저장하고 응답(Accounting Reply) 메시지를 패킷 데이터 서비스 노드로 전송하며, 과정(g)에서 패킷 데이터 서비스 노드는 Ack 메시지를 기지국으로 전송하여 과금 처리가 수행되었음을 알린다.

<71> 과정(h)에서 기지국은 패킷 데이터 서비스 노드를 통해 방송 서버로부터 수신한 방송 데이터를 상기 암호화 키를 가지고 암호화하여 방송 서비스 채널을 통해 단말로 전송한다. 그러면 단말은 상기 수신한 암호화 키를 가지고 상기 방송 데이터를 복호한다.

<72> 보다 구체적으로 설명하면, 기지국 제어기(BSC)는 단말의 등록 메시지에 응답하여 암호화 키를 생성하고 상기 생성된 암호화 키의 정보를 단말로 전송하며, 방송 서버로부터 패킷 데이터 서비스 노드를 통해 제공되는 방송 데이터는 기지국의 제2 계층에 해당하는 기지국 송수신기(BTS)에서 암호화된 후 단말로 전송된다.

<73> 이상에서는 기지국에서 방송 서비스를 위한 암호화 키를 생성하고 방송 데이터를 암호화하는 동작을 설명하였으나, 다른 경우 이러한 동작은 도 7에 도시한 바와 같은 동작에 따라 패킷 데이터 서비스에서 수행될 수 있다.

<74> 도 7은 전형적인 방송 서비스 시스템에서 패킷 데이터 서비스 노드(PDSN)에 의해 단말의 등록을 수행하는 동작을 나타낸 메시지 흐름도이다. 여기에서 단말은 방송 서버로부터 방송 서버와 세션을 연결하기 위해 필요한 방송용 서비스 파라미터를 BSPM을 통해 이미 수신한 것으로 한다.

<75> 상기 도 7을 참조하면, 과정(a)에서 단말은 방송 서비스를 요구하기 위해 기지국으로 등록 메시지를 전송한다. 상기 등록 메시지의 포맷은 앞서 언급한 도 4에 나타낸 바와 같다. 상기 등록 메시지는 단말의 위치를 이동통신 시스템으로 등록함과 동시에 수신하고자 하는 방송 서비스의 종류를 기지국으로 전달하며, 또한 방송 서비스를 위한 암호화 키를 요구하기 위한 것이다. 단말의 위치는 상기 등록 메시지를 수신하여 시스템으로 전달하는 기지국의 식별자에 의하여 알려지며, 단말이 수신하고자 하는 방송 서비스의 종류는 상기 등록 메시지에 포함되는 BCS_ID 필드에 의해 알려진다.

<76> 과정(b)에서 기지국은 단말로부터 BCS_ID를 포함하는 등록 메시지를 최초로 수신하면 단말로부터 방송 서비스가 요구된 것으로 판단하고 자동적으로 Ack 메시지로 응답하는 동시에 상기 단말의 위치 정보를 교환기(도시하지 않음) 또는 AAA 서버로 전달하여 등록한다. 그리고 과정(c)에서 기지국은 현재의 시간으로 설정된 단말의 시간 스탬프(time stamp) 정보와 상기 BCS_ID를 IOS 메시지에 실어 패킷 데이터 서비스 노드로 전송한다.

<77> 과정 (d)에서 패킷 데이터 서비스 노드는 상기 IOS 메시지에 응답하여 단말기 별로 방송 서비스 접속 시간에 대한 정보, 즉 과금 정보를 과금 요구(Accounting Request) 메시지에 실어 AAA 서버로 전송한다. 그러면 과정(e)에서 AAA 서버는 상기 과금 정보를 저장하고 응답(Accounting Reply) 메시지를 패킷 데이터 서비스 노드로 전송한다.

<78> 상기한 과금 처리가 완료된 후, 과정(f)에서 패킷 데이터 서비스 노드는 상기 BCS_ID에 해당하는 방송 서비스를 위해 현재 시점에서 유효한 암호화 키를 생성하고 상기 과금 처리가 성공적으로 수행되었음을 알리는 Ack 메시지에 상기 암호화 키의 정보를 실어 기지국으로 전송한다. 상기 패킷 데이터 서비스 노드는 상기 암호화 키 자체를 전송하거나 또는 상기 암호화 키를 생성하는데 사용되는 생성 정보, 즉 시드를 전송할 수 있다.

<79> 과정(g)에서 기지국은 상기 패킷 데이터 서비스 노드로부터 수신한 상기 암호화 키 또는 상기 생성 정보를 데이터 버스트 메시지(DBM) 또는 암호화 정보 메시지(EIM)에 실어 단말로 전송한다. 도 7에서 암호화 키는 X로 표기되었으며 미리 정해지는 소정의 유효시간을 가진다. 또한 마찬가지로 상기 데이터 버스트 메시지 또는 상기 암호화 정보 메시지는 상기 암호화 키 또는 상기 생성 정보를 적어도 포함하며, 선택적으로 상기 암호화 키의 유효시간을 포함한다.

<80> 과정(h)에서 단말은 상기 암호화 키를 성공적으로 수신하거나 또는 상기 생성 정보를 수신하여 상기 암호화 키를 성공적으로 생성하면 기지국으로 Ack 메시지를 전송하여 상기 암호화

키가 성공적으로 수신되었음을 알린다. 과정(h)에서 패킷 데이터 서비스 노드는 방송 서버로부터 수신한 방송 데이터를 상기 암호화 키를 가지고 암호화하여 기지국을 통해 단말로 전송한다. 그러면 단말은 상기 수신한 암호화 키를 가지고 상기 방송 데이터를 복호한다.

<81> 즉, 기지국은 단말의 등록 메시지에 응답하여 패킷 데이터 서비스 노드로부터 제공받은 암호화 키를 단말로 전송하며, 방송 서버로부터 제공되는 방송 데이터는 패킷 데이터 서비스 노드에서 암호화된 후 기지국을 통해 단말로 전송된다.

<82> 이상에서 설명한 바와 같이 기지국 또는 패킷 데이터 서비스 노드는 단말이 전송하는 매 등록 메시지에 대해서 현재 방송 데이터를 암호화하는데 사용되는 암호화 키나 암호화 키를 만드는데 필요한 암호화 키 또는 암호화 키의 생성 정보(즉 시드 값) 및 암호화 키의 유효시간 등의 정보를 전송한다. 암호화 키를 수신하거나 생성 정보를 통해 암호화 키를 생성한 단말은, 상기 암호화 키의 유효시간이 끝나기 이전에 새로운 등록 과정을 수행하여야 연속적인 방송형 서비스의 수신이 가능하다. 단말의 등록 메시지를 수신한 기지국은 패킷 데이터 서비스 노드를 통해 AAA 서버의 과금 정보를 갱신하여 암호화 키의 유효시간 단위로 시간제 과금을 가능케 한다.

<83> 이상에서 설명한 시간제 과금 방법에서는 단말이 전송하는 매 등록 메시지에 대해서 기지국(BS)과 패킷 제어기(PCF), 패킷 데이터 서비스 노드(PDSN), AAA 서버 간의 과금을 위한 통신과 암호화 키의 전송이 일어난다. 방송형 서비스를 수신 중인 모든 단말들은 방송형 서비스를 수신하는 동안 주기적으로 등록 메시지를 전송하고 각 등록 메시지마다 과금 과정과 암호화 키의 전송 동작이 수행되면, 전체적으로 볼 때 많은 통신량이 발생하게 된다. 게다가, 한 암호화 키의 유효시간이 종료되어 새로운 암호화 키가 사용되기 시작되는 경계 시점에서는 방송

형 서비스를 수신 중인 모든 단말들이 새로운 암호화 키를 수신하기 위해 위치 등록을 수행하고 기지국은 이에 대해서 새로운 암호화 키를 전송하여야 하므로 혼잡 현상이 발생한다.

<84> 과금이나 암호화 키의 갱신은 유효시간 단위로 이루어지므로 위치 등록은 하나의 유효시간 동안 한번만 이루어지면 된다. 따라서 암호화 키의 유효시간 이내에 한 단말로부터 반복하여 수신된 2개 이상의 등록 메시지들에 대해 과금 정보를 갱신하고 등록 절차를 수행하는 것은 불필요한 과정이라 할 수 있다. 따라서 본 발명에서는 단말이 전송하는 등록 메시지를 등록 식별자(Registration ID)로 식별하여 과도한 통신량의 발생을 제한하고, 암호화 키의 유효시간이 끝나는 시점 이전의 소정 시간구간을 유도시간(Skew time)으로 설정하여 새로운 암호화 키의 전송에 따른 혼잡을 방지한다.

<85> 본 발명에 따르면 단말은 기지국이 등록 메시지에 대응하여 전송하는 암호화 정보, 즉 암호화 키(또는 암호화 키의 생성 정보)와 암호화 키의 유효시간 등을 등록 식별자로 구분한다. 이렇게 생성된 등록 식별자는 단말이 전송하는 다음 등록 메시지에 포함되어 기지국으로 전송된다. 등록 식별자가 포함된 등록 메시지를 수신한 기지국은 상기 등록 식별자가 이미 전송한 암호화 정보에 대한 것인지를 판단할 수 있다. 만약 앞서 전송했던 암호화 정보의 것과 일치하는 등록 식별자가 수신되었을 경우 기지국은 과금 정보 갱신과 단말에 대한 암호화 정보 갱신에 필요한 모든 절차를 생략할 수 있다.

<86> 등록 메시지에 포함되는 등록 식별자는 다양하게 생성될 수 있으며 여기에서는 바람직한 실시예로서 암호화 키의 관련 정보를 이용하는 방법을 개시한다. 암호화 키의 관련 정보로는 암호화 키 자체, 암호화 키의 생성 정보(즉 시드), 암호화 키의 해시(Hash) 값 등이 있다. 단말로부터의 등록 메시지를 수신한 기지국은 상기 등록 메시지에 포함된 암호화 키나 관련 정보

가 현재 유효한 암호화 키의 것과 동일한지 판단하여 과금 및 암호화 정보의 전송이 필요한지 판단한다.

<87> 단말이 암호화 키로부터 해시 값을 생성하여 등록 메시지에 실어 전송하는 경우, 해시 값은 일반적으로 입력 값보다 짧은 길이를 가지므로, 비교적 큰 크기의 암호화 키 자체 또는 암호화 키의 생성 정보를 등록 메시지에 삽입하여 전송하는 경우에 비하여 효율적인 전송이 가능하다. 알려진 바와 같이 해시 함수는 결과 값에 대해서 입력 값을 찾기 어려우며 동일한 결과 값을 가지는 서로 다른 입력 값들을 찾기 어려운 성질을 가지고 있다. 따라서 단말이 암호화 키의 해시 값을 전송하였을 때, 기지국은 충분히 높은 확률로 현재 암호화 키의 해시 값과의 동일성 여부를 판단할 수 있다.

<88> 하기에 모듈로(Modulo)를 사용하는 대표적인 해시 함수의 예를 개시하였다.

<89> $f(x) = x \bmod 16$

<90> 상기 수식은 8 비트의 암호화 키로부터 4 비트의 해시 값을 생성하는 해시 함수이다. 여기서 x는 수신한 암호화 키(X key) 또는 수신한 시드를 이용하여 생성한 암호화 키이며 f(x)는 x에 대응하는 결과로 길이 4 비트의 해시 값이다.

<91> 도 8은 본 발명의 일 실시예에 따라 암호화 키의 관련 정보를 포함하는 등록 메시지의 포맷을 나타낸 것으로서, 여기에서 암호화 키는 8비트이고 암호화 키의 관련 정보로는 4비트의 해시 값을 사용한다. ENCRYPTION_KEY_HASH_INCL 필드가 1의 값을 가질 때, 암호화 키의 해시 값은 ENCRYPTION_KEY_HASH 필드를 통해 단말로부터 기지국으로 전송된다.

<92> 암호화 키의 해시 값을 전송하는 경우, 암호화 키 또는 암호화 키의 생성 정보를 전송하는 경우보다 적은 비트 수의 등록 식별자를 사용하여 등록 메시지의 길이를 줄일 수 있으나,

낮은 확률이나마 해시 값간의 충돌이 일어날 가능성이 있다. 즉, 단말과 기지국이 서로 다른 암호화 키를 가지고 동일한 해시 값을 생성할 수 있다. 이런 경우 기지국은 단말이 이미 유효한 암호화 키를 가지고 있는 것으로 판단하지만, 단말은 현재 유효한 암호화 키를 알지 못하여 방송 데이터를 수신할 수 없다. 이런 경우를 방지하기 위하여 패킷 데이터 서비스 노드는 암호화 키를 생성할 때, 이전에 사용하였던 암호화 키와 해시 값이 다른 암호화 키를 선택하여 생성한다.

<93> 도 9는 본 발명에 따라 암호화 키의 해시 값을 사용하여 등록을 수행하는 방송 서비스 동작을 나타낸 메시지 흐름도이다. 여기에서 방송형 서비스의 암호화 키는 패킷 데이터 서비스 노드에서 생성되고 기지국은 패킷 데이터 서비스 노드가 생성한 암호화 키를 저장하고 있다가, 단말로부터 등록 메시지를 수신하여 과금 및 암호화 키 전송 여부를 판단한다. 또한 단말은 방송 서버로부터 방송 서버와 세션을 연결하기 위해 필요한 방송용 서비스 파라미터를 BSPM을 통해 이미 수신하여 저장하고 있는 것으로 한다.

<94> 상기 도 9를 참조하면, 과정(a)에서 단말은 방송 서비스를 요구하기 위해 기지국으로 제1 등록 메시지를 전송한다. 상기 제1 등록 메시지는 단말의 위치를 이동통신 시스템으로 등록함과 동시에 최초에 방송 서비스를 요구하기 위한 것이므로 등록 식별자를 포함하지 않으며 그 포맷은 앞서 언급한 도 4에 나타낸 바와 같다. 단말의 위치는 상기 제1 등록 메시지를 수신하여 시스템으로 전달하는 기지국의 식별자에 의하여 알려지며, 단말이 수신하고자 하는 방송 서비스의 종류는 상기 등록 메시지에 포함되는 BCS_ID 필드에 의해 알려진다.

<95> 과정(b)에서 기지국은 단말로부터 등록 식별자를 포함하지 않는 상기 제1 등록 메시지를 수신하면 자동적으로 Ack 메시지로 응답하는 동시에 상기 단말의 위치 정보를 교환기(도시하지 않음) 또는 AAA 서버로 전달하여 등록한다. 그리고 과정(c)에서 기지국은 현재의 시간으로 설

정된 단말의 시간 스탬프(time stamp) 정보와 상기 BCS_ID를 IOS 메시지에 실어 패킷 데이터 서비스 노드로 전송한다.

<96> 과정 (d)에서 패킷 데이터 서비스 노드는 상기 IOS 메시지에 응답하여 단말기 별로 방송 서비스 접속 시간에 대한 정보, 즉 과금 정보를 과금 요구(Accounting Request) 메시지에 실어 AAA 서버로 전송한다. 그러면 과정(e)에서 AAA 서버는 상기 과금 정보를 저장하고 응답(Accounting Reply) 메시지를 패킷 데이터 서비스 노드로 전송한다.

<97> 상기한 과금 처리가 완료된 후, 과정(f)에서 패킷 데이터 서비스 노드는 상기 BCS_ID에 해당하는 방송 서비스를 위해 현재 시점에서 유효한 암호화 키 X를 생성하고 상기 과금 처리가 성공적으로 수행되었음을 알리는 Ack 메시지에 상기 암호화 키를 실어 기지국으로 전송한다. 상기 패킷 데이터 서비스 노드는 상기 암호화 키 전체를 전송하거나 또는 상기 암호화 키를 생성하는데 사용되는 생성 정보를 전송할 수 있다. 과정(g)에서 기지국은 상기 패킷 데이터 서비스 노드로부터 수신한 상기 암호화 키 또는 상기 생성 정보를 데이터 버스트 메시지(DBM)에 실어 단말로 전송한다.

<98> 과정(h)에서 단말은 상기 암호화 키를 성공적으로 수신하거나 또는 상기 생성 정보를 수신하여 상기 암호화 키를 성공적으로 생성하면 기지국으로 Ack 메시지를 전송하여 상기 암호화 키가 성공적으로 수신되었음을 알린다. 이때 단말은 상기 암호화 키의 수신에 대응하는 등록 식별자로서 상기 암호화 키의 해시 값을 생성하여 저장한다. 과정(i)에서 패킷 데이터 서비스 노드는 방송 서버로부터 수신한 방송 데이터를 상기 암호화 키를 가지고 암호화하여 기지국을 통해 단말로 전송한다. 그러면 단말은 상기 수신한 암호화 키를 가지고 상기 방송 데이터를 복호한다.

<99> 과정(j)에서 단말은 주기적인 등록 타이머가 만기되거나 또는 다른 등록 요구 조건에 따른 위치 등록을 수행하기 위해 제2 등록 메시지를 생성하여 기지국으로 전송한다. 여기서 상기 제2 등록 메시지는 상기 과정(h)에서 단말에 의해 생성된 암호화 키의 해시 값을 나타내는 등록 식별자를 포함한다. 기지국은 상기 제2 등록 메시지에 포함된 상기 해시 값에 의해 과금 및 암호화 키의 전송 여부를 판단한다. 즉, 기지국은 기 수신된 등록 식별자가 존재하는지 및 상기 등록 식별자가 기 수신된 등록 식별자와 일치하는지를 판단한다. 만일 일치하면 유효시간 내에 두 번 이상의 등록이 이루어진 것으로 판단하여 상기 제2 등록 메시지를 무시한다.

<100> 마찬가지로 과정(k)에서 유효시간 내에 다시 제3 등록 메시지가 수신되면 기지국은 상기 제3 등록 메시지를 무시한다. 여기에서 상기 제2 및 제3 등록 메시지를 무시한다는 것은 기지국에서 상기 제2 및 제3 등록 메시지에 응답하여 과금 또는 암호화 정보의 전송을 수행하지 않음을 의미하며, 상기 제2 및 제3 등록 메시지에 대응하는 Ack 메시지는 자동적으로 단말에게 전송된다.

<101> 도 9에서 단말이 동일한 암호화 키를 가지고 방송 서비스를 수신하는 시간구간은 음영으로 표시하였으며, 상기 표시한 구간에서는 단말이 추가의 등록 메시지들을 전송하더라도 과금 및 추가적인 암호화 키의 전송이 일어나지 않는다.

<102> 이상과 같이 암호화 키의 해시 값에 의해 등록 메시지를 구별하는 경우, 암호화 키 또는 암호화 키의 생성 정보를 전송하는 경우보다 적은 비트 수의 등록 식별자를 사용하여 등록 메시지의 길이를 줄일 수 있으나, 낮은 확률이나마 해시 값들간의 충돌이 일어날 가능성이 있다. 즉, 단말과 기지국이 서로 다른 암호화 키들을 가지고 동일한 해시 값들을 생성할 수 있다. 이런 경우 기지국은 단말이 이미 유효한 암호화 키를 가지고 있는 것으로 판단하지만, 실제로 단말은 현재 유효한 암호화 키를 알지 못하여 방송 데이터를 수신할 수 없다. 이런 경우를 방지

하기 위하여 패킷 데이터 서비스 노드는 암호화 키를 생성할 때, 이전에 사용하였던 암호화 키와 해시 값이 다른 암호화 키를 선택하여 생성한다.

<103> 본 발명의 변형된 실시예에서 기지국은 단말에게 암호화 키를 전송할 때 상기 암호화 키에 대해 부여된 시퀀스 번호를 함께 전송한다. 그러면 단말은 등록 메시지에 기 수신한 암호화 키의 시퀀스 번호를 삽입하여 전송한다. 기지국은 단말로부터 수신한 등록 메시지의 시퀀스 번호가 현재 유효한 암호화 키의 시퀀스 번호와 동일할 경우 단말의 암호화 정보가 여전히 유효하고 판단한다. 단말로부터 수신한 등록 메시지의 시퀀스 번호가 기지국의 유효한 암호화 키의 시퀀스 번호와 다를 경우, 기지국은 과금 정보를 갱신하고 새로운 암호화 정보를 전송한다.

<104> 본 발명의 변형된 실시예에서 단말은 방송 서비스를 수신하기 위해 최초로 전송한 등록 메시지에 대응하여 수신한 암호화 정보에 대해 시퀀스 번호 0을 부여하고, 이후 새로운 암호화 정보가 수신될 때마다 시퀀스 번호를 1씩 추가한다. 상기 시퀀스 번호는 기지국으로 전송되는 등록 메시지에 삽입된다. 기지국은 단말로부터 최초로 수신한 등록 메시지에 대응하여 전송한 암호화 정보에 대해 시퀀스 번호 0을 부여하고, 이후 새로운 암호화 정보를 전송할 때마다 시퀀스 번호를 1씩 추가한다. 단말로부터 등록 메시지가 수신되면, 기지국은 상기 등록 메시지에 포함된 시퀀스 번호가 해당 단말의 시퀀스 번호와 일치하는지를 확인하여 해당 단말이 가지고 있는 암호화 키의 유효성 여부를 판단한다.

<105> 도 10은 본 발명의 변형된 실시예에 따라 암호화 키의 시퀀스 번호를 포함하는 등록 메시지의 포맷을 나타낸 것으로서, 여기에서 암호화 키의 시퀀스 번호는 2비트의 길이를 가지며 0 ~ 3 사이의 값을 표현할 수 있다. 상기 암호화 키의 시퀀스 번호는 ENCRYPTION_KEY_SEQ_INCL 필드가 1의 값을 가질 때, 등록 메시지의 ENCRYPTION_KEY_SEQ 필드를 통해 전송된다.

<106> 마찬가지로 단말은 암호화 키의 수신을 위해 최초로 등록 메시지를 전송할 때는 ENCRYPTION_KEY_SEQ_INCL 필드를 0으로 설정하여 암호화 키의 시퀀스 정보를 생략하며, 암호화 키의 시퀀스 번호를 포함하지 않는 등록 메시지를 수신한 기지국은 현재의 유효한 암호화 정보를 전송한다.

<107> 본 발명의 다른 변형된 실시예에서 단말은 방송 서비스의 수신을 요구하기 위해 최초로 전송하는 등록 메시지에 암호화 정보의 전송을 요구하는 암호화 키 요구 비트 필드를 삽입한다. 기지국은 암호화 키 요구 비트가 1로 설정된 등록 메시지를 받으면 암호화 정보로서 암호화 키 또는 암호화 키의 생성 정보와 암호화 키의 유효시간을 단말에게 전송한다. 단말은 상기 암호화 키의 유효시간을 참조하여, 상기 유효시간 동안에는 암호화 키 요구 비트를 0으로 설정한 등록 메시지를 전송하고, 상기 유효시간이 종료되면 암호화 키 요구 비트를 1로 설정한 등록 메시지를 전송한다. 방송 서비스가 시작된 이후 기지국은 단말로부터 수신한 등록 메시지의 암호화 키 요구 비트가 1일 때에만 과금 정보를 갱신하고 암호화 정보를 전송한다.

<108> 도 11은 본 발명의 다른 변형된 실시예에 따라 암호화 키 요구 비트를 포함하는 등록 메시지의 포맷을 나타낸 것으로서, 도시한 바와 같이 단말은 한 비트의 ENCRYPTION_KEY_REQ 필드를 통해 새로운 암호화 키를 요구할 수 있다.

<109> 도 12는 본 발명에 따라 등록 식별자를 사용하는 단말의 등록 동작을 나타낸 흐름도이다.

<110> 상기 도 12를 참조하면, 방송 서비스 중인 단말은 과정(100)에서 위치등록을 수행하는 주기에 도달하였는지 또는 미리 정해진 위치등록 조건이 만족되어 위치등록을 수행하여야 하는지를 확인한다. 만일 위치등록을 수행하여야 하는 것으로 판단되면 단말은 과정(110)에서 등록 메시지를 생성하고 과정(120)에서 상기 등록 메시지에 현재의 유효한 암호화 키에 대한 등록

식별자를 삽입하며, 과정(130)에서 상기 등록 식별자를 포함하는 상기 등록 메시지를 기지국으로 전송한다. 상기 등록 식별자는 앞서 언급한 암호화 키의 해시 값, 시퀀스 번호 또는 암호화 키 요구 비트이다.

<111> 과정(140)에서 상기 등록 메시지에 대응하는 암호화 정보가 수신되면, 과정(150)에서 단말은 상기 암호화 정보를 방송 서비스를 위해 저장하는 한편 상기 등록 식별자를 갱신한다. 즉, 단말은 상기 암호화 정보에 포함된 암호화 키를 가지고 새로운 해시 값을 생성하거나, 시퀀스 번호를 1만큼 증가시키거나, 유효시간에 따라 암호화 키 요구 비트를 1 또는 0으로 설정한다. 상기 과정(140)에서 암호화 정보가 수신되지 않으면 과정(100)으로 복귀한다.

<112> 도 13은 본 발명에 따라 등록 식별자를 사용하는 기지국의 등록 동작을 나타낸 흐름도이다.

<113> 상기 도 13을 참조하면, 기지국은 과정(200)에서 방송 서비스 중인 단말로부터 등록 메시지가 수신되는지를 확인하고, 만일 수신되었으면 과정(210)에서 상기 수신된 등록 메시지에 등록 식별자가 포함되어 있는지를 확인한다. 만일 등록 식별자가 포함되어 있으면 과정(220)으로 진행하고 그렇지 않으면 과정(230)으로 진행한다.

<114> 상기 과정(220)에서 기지국은 상기 등록 식별자에 따라 단말로부터 암호화 정보가 요구되는지를 확인한다. 즉, 상기 등록 메시지에 포함된 해시 값이 현재 유효한 암호화 키의 해시 값과 일치하지 않거나, 상기 등록 메시지에 포함된 시퀀스 번호가 해당 단말에 대해 가지고 있는 시퀀스 번호와 일치하지 않거나, 상기 등록 메시지에 포함된 암호화 키 요구 비트의 값이 1이면, 기지국은 새로운 암호화 정보가 요구된 것으로 판단하여 과정(230)으로 진행하고 그렇지 않으면 기지국은 단말에게 Ack 메시지를 전달하고 과정(200)으로 복귀한다.

<115> 기지국은 과정(230)에서 현재 유효한 암호화 키 또는 암호화 키의 생성 정보를 적어도 포함하고 선택적으로 상기 암호화 키의 유효시간을 포함하는 암호화 정보를 생성하여 단말로 전송하고, 과정(240)에서 단말에 대한 과금 정보를 갱신하여 패킷 데이터 서비스 노드를 통해 AAA 서버로 전송한다.

<116> 이상에서 설명한 바와 같이, 단말은 소정의 유효시간을 가지는 암호화 키를 사용하여 방송 데이터를 복호한다. 연속적인 방송 서비스를 위해서 단말은 암호화 키의 유효시간이 만료되기 이전에 새로운 암호화 키를 요구하는 등록 메시지를 전송한다. 상기 등록 메시지는 앞서 언급한 바와 같은 등록 식별자로서 암호화 키의 관련 정보, 시퀀스 번호, 암호화 키 요구 비트를 포함하는 것이다. 기지국은 상기 등록 메시지에 응답하여 새로운 암호화 정보를 단말에게 전송한다.

<117> 암호화 키는 해당 유효시간 내에서 한 기지국의 서비스영역 내에서 방송 서비스를 수신하는 다수의 단말들에 의해 공유되는 것이므로, 유효시간의 경계시점에서는 방송 서비스를 수신 중인 모든 단말들이 등록 메시지들을 전송하고 기지국은 등록 메시지를 전송한 각 단말에게 일일이 새로운 암호화 정보를 전송해야 한다. 이러한 과정은 한 순간에 많은 메시지의 집중을 야기시켜 정상적인 시스템의 동작을 방해한다. 이런 문제점을 보안하기 위해 본 발명에서는 암호화 키의 유효시간이 종료되기 이전에 유도시간(Skew time)을 설정한다.

<118> 기지국은 해당하는 서비스영역 내에서 방송 서비스 중인 모든 단말들의 등록 메시지 송신 주기 중 최대 주기보다 큰 시간으로 유도시간을 설정한다. 그러면 모든 단말들은 유도시간 내에 적어도 한 번은 등록 메시지를 전송하게 된다. 기지국은 암호화 키의 유효시간이 종료되기 이전 유도시간 동안에 등록 메시지를 전송한 단말에게, 현재의 유효한 암호화 정보와 함께

다음 암호화 키의 정보를 전송한다. 단말은 상기 현재 암호화 키의 유효시간이 종료된 이후 상기 다음 암호화 키를 이용하여 방송 데이터를 연속적으로 수신할 수 있다.

<119> 도 14는 본 발명에 따라 유도시간을 사용하는 방송 서비스 절차를 나타낸 메시지 흐름도로서, 여기에서 단말은 기지국을 통해 방송 데이터를 이미 수신하고 있으며 등록 식별자로서 암호화 키의 해시 값을 포함하는 등록 메시지를 주기적으로 또는 비주기적으로 전송한다.

<120> 상기 도 14를 참조하면, 과정(a)에서 단말은 기지국을 통해 수신하는 방송 데이터를 현재의 유효한 암호화 키를 가지고 복호한다. 과정(b)에서 단말은 주기적인 등록 타이머가 만기되거나 또는 다른 등록 요구 조건에 따른 위치 등록을 수행하기 위해 제1 등록 메시지를 생성하여 기지국으로 전송한다. 여기서 상기 제1 등록 메시지는 상기 암호화 키의 해시 값을 나타내는 등록 식별자를 포함한다. 기지국은 상기 제1 등록 메시지가 미리 설정된 유도시간 이전에 수신된 것임을 확인하고 상기 제1 등록 메시지를 무시한다. 즉 기지국은 단말에게 Ack 메시지를 전송할 뿐 상기 제1 등록 메시지에 따른 암호화 키 전송 및 과금 처리 등의 절차를 수행하지 않는다.

<121> 다른 경우, 기지국은 상기 제1 등록 메시지에 포함된 등록 식별자 또는 암호화 키 요구 비트에 따라 상기 제1 등록 메시지를 무시한다. 또 다른 경우 기지국은 상기 제1 등록 메시지가 미리 설정된 유도시간 이전에 수신된 것임을 확인하면, 상기 제1 등록 메시지에 포함된 등록 식별자 또는 암호화 키 요구 비트에 따라 상기 제1 등록 메시지를 무시한다.

<122> 과정(c)에서 현재 암호화 키의 유효시간이 종료되기 이전 유도시간 동안에 단말로부터 제2 등록 메시지가 수신되면, 기지국은 자동적으로 Ack 메시지로 응답하는 동시에 상기 단말의 위치 정보를 교환기(도시하지 않음) 또는 AAA 서버로 전달하여 등록한다. 그리고 과정(d)에서

기지국은 현재의 시간으로 설정된 단말의 시간 스탬프 정보와 해당하는 BCS_ID를 IOS 메시지에 실어 패킷 데이터 서비스 노드로 전송한다.

<123> 과정 (e)에서 패킷 데이터 서비스 노드는 상기 IOS 메시지에 응답하여 단말기 별로 방송 서비스 접속 시간에 대한 정보, 즉 과금 정보를 과금 요구 메시지에 실어 AAA 서버로 전송한다. 그러면 과정(f)에서 AAA 서버는 상기 과금 정보를 저장하고 응답 메시지를 패킷 데이터 서비스 노드로 전송한다.

<124> 상기한 과금 처리가 완료된 후, 과정(g)에서 패킷 데이터 서비스 노드는 상기 BCS_ID에 해당하는 방송 서비스를 위해 현재 사용되는 암호화 키(또는 생성 정보)와 다음으로 사용될 암호화 키(또는 생성 정보)를, 상기 과금 처리가 성공적으로 수행되었음을 알리는 Ack 메시지에 실어 기지국으로 전송한다. 과정(h)에서 기지국은 상기 패킷 데이터 서비스 노드로부터 수신한 상기 현재 및 다음 암호화 키와 그 유효시간에 대한 정보를 데이터 버스트 메시지(DBM) 또는 암호화 정보 메시지(EIM)에 실어 단말로 전송하고, 과정(i)에서 그에 대한 응답으로서 Ack 메시지를 수신한다.

<125> 이상과 같이 기지국은 유도시간 동안 수신된 단말의 등록 메시지에 대해 과금 정보를 갱신하고 현재 암호화 키와 다음 암호화 키를 단말에게 전송한다. 이로써 단말은 현재 암호화 키의 유효시간이 종료되면 다음 암호화 키를 사용하여 연속적으로 방송형 서비스를 수신할 수 있다. 등록 메시지 전송은 단말이 최초에 방송 서비스를 개시한 시간으로부터 시작하여 주기적으로 이루어지는 것이므로 유도시간 내에서 충분히 랜덤하다고 볼 수 있다. 따라서 유도시간 내에서 등록 메시지들의 집중에 따른 혼잡 상황의 발생을 피할 수 있다.

<126> 도 15는 본 발명에 따라 현재 암호화 키 및 다음 암호화 키를 포함하는 데이터 버스트 메시지의 포맷을 나타낸 것으로서, 상기 도 15를 참조하여 데이터 버스

트 메시지의 주요 필드들을 살펴보면, BURST_TYPE 필드는 포함되는 데이터의 종류를 나타내며, NUM_FIELDS 필드는 이어지는 CHARi 필드에 포함되는 필드들의 개수를 나타낸다. 상기 BURST_TYPE 필드가 암호화 키를 전송하는 DBM 유형을 나타내는 미리 정해진 값을 가지는 경우의 CHARi 필드의 데이터 구조(Data Structure)를 도 15의 하부에 나타내었다.

<127> 도시한 CHARi 필드에서, NUM_BCS_SESSION 필드는 방송 서비스를 위해 연결된 세션 개수를 나타내고, 상기 세션 개수에 따라 방송 서비스를 위한 필드들이 이어진다. 방송 서비스를 위한 필드들로는 요구되는 방송 서비스의 내용을 나타내는 BCS_ID 필드와, 현재 암호화 키 또는 현재 암호화 키의 생성 정보를 나타내는 ENCRYPTION_KEY 필드와, 상기 현재 암호화 키의 유효시간을 나타내는 ENCRYPTION_KEY_LIFETIME 필드와, 다음 암호화 키의 정보가 포함되는지의 여부를 나타내는 NEXT_ENCRYPTION_KEY_INCL 필드와, 다음 암호화 키 또는 다음 암호화 키의 생성 정보를 나타내는 NEXT_ENCRYPTION_KEY 필드와, 상기 다음 암호화 키의 유효시간을 나타내는 NEXT_ENCRYPTION_KEY_LIFE_TIME 필드가 있다. 또한, 기지국이 단말에게 등록 식별자로서 시퀀스 번호를 부여하는 경우, 기지국은 CHARi 필드의 ENCRYPTION_KEY_SEQ_INCL 필드를 1로 설정하고 ENCRYPTION_KEY_SEQ 필드를 통해 상기 부여된 시퀀스 번호를 단말에게 전송한다.

<128> 다른 경우, 상기 BURST_TYPE 필드는 통상의 데이터 버스트 유형을 나타내는 값으로 설정되고 CHARi 필드는 패킷 데이터 서비스 노드로부터 단말로 전달되는 IP 패킷을 담을 수 있다. 이 경우 단말은 상기 IP 패킷의 내용을 분석하여 현재 및 다음 암호화 키와 그 유효시간들 등의 방송 서비스 관련 정보들을 추출한다.

<129> 도 16은 본 발명에 따라 현재 암호화 키 및 다음 암호화 키를 포함하는 암호화 정보 메시지의 포맷을 나타낸 것으로서, 상기 도 16을 참조하여 암호화 정보 메시지의 주요 필드들을 살펴보면, NUM_BCS_SESSION 필드는 방송 서비스를 위해 연결된 세션 개수를 나타내고, 상기 세

션 개수에 따라 방송 서비스를 위한 필드들이 이어진다. 방송 서비스를 위한 필드들로는 요구되는 방송 서비스의 내용을 나타내는 BCS_ID 필드와, 현재 암호화 키 또는 현재 암호화 키의 생성 정보를 나타내는 ENCRYPTION_KEY 필드와, 상기 현재 암호화 키의 유효시간을 나타내는 ENCRYPTION_KEY_LIFETIME 필드와, 다음 암호화 키의 정보가 포함되는지의 여부를 나타내는 NEXT_ENCRYPTION_KEY_INCL 필드와, 다음 암호화 키 또는 다음 암호화 키의 생성 정보를 나타내는 NEXT_ENCRYPTION_KEY 필드와, 상기 다음 암호화 키의 유효시간을 나타내는 NEXT_ENCRYPTION_KEY_LIFE_TIME 필드가 있다.

<130> 마찬가지로, 기지국이 단말에게 등록 식별자로서 시퀀스 번호를 부여하는 경우, 기지국은 ENCRYPTION_KEY_SEQ_INCL 필드를 1로 설정하고 ENCRYPTION_KEY_SEQ 필드를 통해 상기 부여된 시퀀스 번호를 단말에게 전송한다.

<131> 한편 본 발명의 상세한 설명에서는 구체적인 실시예에 관해 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 그러므로 본 발명의 범위는 설명된 실시예에 국한되지 않으며, 후술되는 특허청구의 범위뿐만 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

【발명의 효과】

<132> 이상에서 상세히 설명한 바와 같이 동작하는 본 발명에 있어서, 개시되는 발명중 대표적인 것에 의하여 얻어지는 효과를 간단히 설명하면 다음과 같다.

<133> 본 발명은 단말의 위치 등록에 대하여 방송 서비스를 위한 암호화 키를 전송하고 과금을 수행에 있어서 불필요한 암호화 키의 전송과 과금 처리로 인한 시스템 성능의 저하를 방지한다. 또한 본 발명은 암호화 키의 유효시간이 만기되기 직전에 단말들의 등록 메시지들이 집중되는 문제점을 해소할 수 있는 효과가 있다.

【특허청구범위】

【청구항 1】

무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 상기 단말에서 방송 서비스를 제공받는 방법에 있어서,

상기 이동통신 시스템에 방송 서비스의 지속적인 제공을 요청하기 위해 기 수신한 암호화 키를 식별하는 등록 식별자를 포함하는 등록 메시지를 생성하여 상기 기지국으로 전송하는 과정과,

상기 등록 메시지에 응답하여 방송 서비스를 위해 암호화 키를 포함하는 암호화 정보 메시지를 수신하는 과정과,

방송 서비스 채널을 통해 상기 기지국으로부터 수신한 방송 데이터를 복호화하기 위해 상기 암호화 정보 메시지에 포함된 암호화 키를 저장하고, 상기 암호화 키에 대응하여 상기 등록 식별자를 갱신하는 과정을 포함하는 것을 특징으로 하는 상기 방법.

【청구항 2】

제 1 항에 있어서, 상기 암호화 키는 소정의 유효시간을 가지는 것을 특징으로 하는 상기 방법.

【청구항 3】

제 1 항에 있어서, 상기 등록 식별자는, 상기 단말에 의해 상기 암호화 키를 가지고 생성된 해시 값 또는 상기 암호화 키에 대해 부여된 시퀀스 번호인 것을 특징으로 하는 상기 방법.

【청구항 4】

제 1 항에 있어서, 상기 암호화 정보 메시지는, 상기 기지국에 의해 상기 암호화 키에 대해 부여된 등록 식별자를 더 포함하는 것을 특징으로 하는 상기 방법.

【청구항 5】

제 4 항에 있어서, 상기 등록 식별자는, 상기 암호화 키에 대해 부여된 시퀀스 번호인 것을 특징으로 하는 상기 방법.

【청구항 6】

무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 상기 기지국에 의해 상기 단말에게 방송 서비스를 제공하는 방법에 있어서,

상기 단말로부터 상기 이동통신 시스템에 방송 서비스의 제공을 요청하기 위한 등록 메시지를 수신하는 과정과,

상기 등록 메시지에 따라 상기 단말로부터 암호화 키가 요구되는지를 판단하는 과정과,

상기 암호화 키가 요구되는 것으로 판단되면, 방송 서비스를 위한 암호화 키를 포함하는 암호화 정보 메시지를 상기 단말로 전송하는 과정을 포함하는 것을 특징으로 하는 상기 방법.

【청구항 7】

제 6 항에 있어서, 상기 암호화 키는 소정의 유효시간을 가지는 것을 특징으로 하는 상기 방법.

【청구항 8】

제 6 항에 있어서, 상기 판단하는 과정은,

상기 등록 메시지에 상기 단말에서 방송 서비스를 위해 사용중인 암호화 키를 식별하는 등록 식별자가 포함되어 있는지를 판단하고, 상기 등록 식별자에 따라 상기 단말로부터 암호화 키가 요구되는지를 판단하는 것을 특징으로 하는 상기 방법.

【청구항 9】

제 8 항에 있어서, 상기 등록 식별자는, 상기 단말에 의해 상기 기 사용중인 암호화 키를 가지고 생성된 해시 값 또는 상기 기 사용중인 암호화 키에 대해 부여된 시퀀스 번호인 것을 특징으로 하는 상기 방법.

【청구항 10】

제 9 항에 있어서, 상기 등록 식별자가 상기 단말로부터 기 수신한 등록 식별자와 일치하지 않으면 상기 단말로부터 암호화 키가 요구된 것으로 판단하는 것을 특징으로 하는 상기 방법.

【청구항 11】

제 6 항에 있어서, 상기 등록 식별자는, 상기 기지국에 의해 상기 암호화 키에 대해 부여된 시퀀스 번호인 것을 특징으로 하는 상기 방법.

【청구항 12】

제 6 항에 있어서, 상기 암호화 정보 메시지는, 상기 기지국에 의해 상기 암호화 키에 대해 부여된 시퀀스 번호를 더 포함하는 것을 특징으로 하는 상기 방법.

【청구항 13】

제 6 항에 있어서, 상기 암호화 키가 요구되지 않는 것으로 판단되면, 상기 등록 메시지에 대응하는 응답 메시지를 상기 단말로 전송하는 과정을 더 포함하는 것을 특징으로 하는 상기 방법.

【청구항 14】

무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 상기 단말에서 방송 서비스를 제공받는 방법에 있어서,

상기 이동통신 시스템에 방송 서비스의 제공을 요청하기 위해 암호화 키를 요구하는 암호화 키 요구 비트를 포함하는 등록 메시지를 생성하여 상기 기지국으로 전송하는 과정과,

상기 등록 메시지에 응답하여 방송 서비스를 위해 암호화 키와 상기 암호화 키의 유효시간을 포함하는 암호화 정보 메시지를 수신하는 과정과,

방송 서비스 채널을 통해 상기 기지국으로부터 수신한 방송 데이터를 복호화하기 위해 상기 암호화 정보 메시지에 포함된 암호화 키와 상기 암호화 키의 유효시간을 저장하는 과정을 포함하는 것을 특징으로 하는 상기 방법.

【청구항 15】

제 14 항에 있어서, 상기 암호화 키를 가지고 방송 서비스를 진행하는 도중 상기 암호화 키의 유효시간이 종료되면, 방송 서비스를 위한 새로운 암호화 키를 요구하는 등록 메시지를 생성하여 상기 기지국으로 전송하는 과정을 더 포함하는 것을 특징으로 하는 상기 방법.

【청구항 16】

무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 상기 기지국에 의해 상기 단말에게 방송 서비스를 제공하는 방법에 있어서,

상기 단말로부터 상기 이동통신 시스템에 방송 서비스의 제공을 요청하기 위한 등록 메시지를 수신하는 과정과,

상기 등록 메시지에 방송 서비스를 위한 암호화 키를 요구하는 암호화 키 요구 비트가 포함되어 있는지를 판단하는 과정과,

상기 암호화 키 요구 비트가 포함되어 있으면, 방송 서비스를 위한 암호화 키와 상기 암호화 키의 유효시간을 포함하는 암호화 정보 메시지를 상기 단말로 전송하는 과정을 포함하는 것을 특징으로 하는 상기 방법.

【청구항 17】

무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 상기 단말에서 방송 서비스를 제공받는 방법에 있어서,

소정 유효시간을 가지는 암호화 키를 가지고 방송 서비스를 진행하는 도중 미리 정해지는 위치등록 조건이 만족될 때 상기 이동통신 시스템에 방송 서비스의 계속적인 제공을 요청하기 위한 등록 메시지를 생성하여 상기 기지국으로 전송하는 과정과,

상기 등록 메시지에 응답하여 방송 서비스를 위해 다음 암호화 키와 상기 다음 암호화 키의 유효시간을 포함하는 암호화 정보 메시지를 수신하는 과정과,

현재 암호화 키를 가지고 방송 서비스를 수신하면서 상기 현재 암호화 키의 유효시간이 종료되었는지를 판단하는 과정과,

상기 현재 암호화 키의 유효시간이 종료되었으면 상기 다음 암호화 키를 가지고 연속적으로 방송 서비스를 수신하는 과정을 포함하는 것을 특징으로 하는 상기 방법.

【청구항 18】

제 17 항에 있어서, 상기 암호화 정보 메시지는, 현재 유효한 암호화 키와 상기 현재 암호화 키의 유효시간을 더 포함하는 것을 특징으로 하는 상기 방법.

【청구항 19】

무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 상기 기지국에 의해 상기 단말에게 방송 서비스를 제공하는 방법에 있어서,

소정 유효시간을 가지는 암호화 키를 가지고 방송 서비스를 진행하는 도중, 상기 단말로부터 상기 이동통신 시스템에 방송 서비스의 계속적인 제공을 요청하기 위한 등록 메시지를 수신하는 과정과,

상기 등록 메시지가 상기 암호화 키의 유효시간이 종료되기 이전 미리 정해진 유도시간 내에 수신된 것으로 판단되면, 방송 서비스를 위해 다음 암호화 키와 상기 다음 암호화 키의

유효시간을 포함하는 암호화 정보 메시지를 상기 단말로 전송하는 과정을 포함하는 것을 특징으로 하는 상기 방법.

【청구항 20】

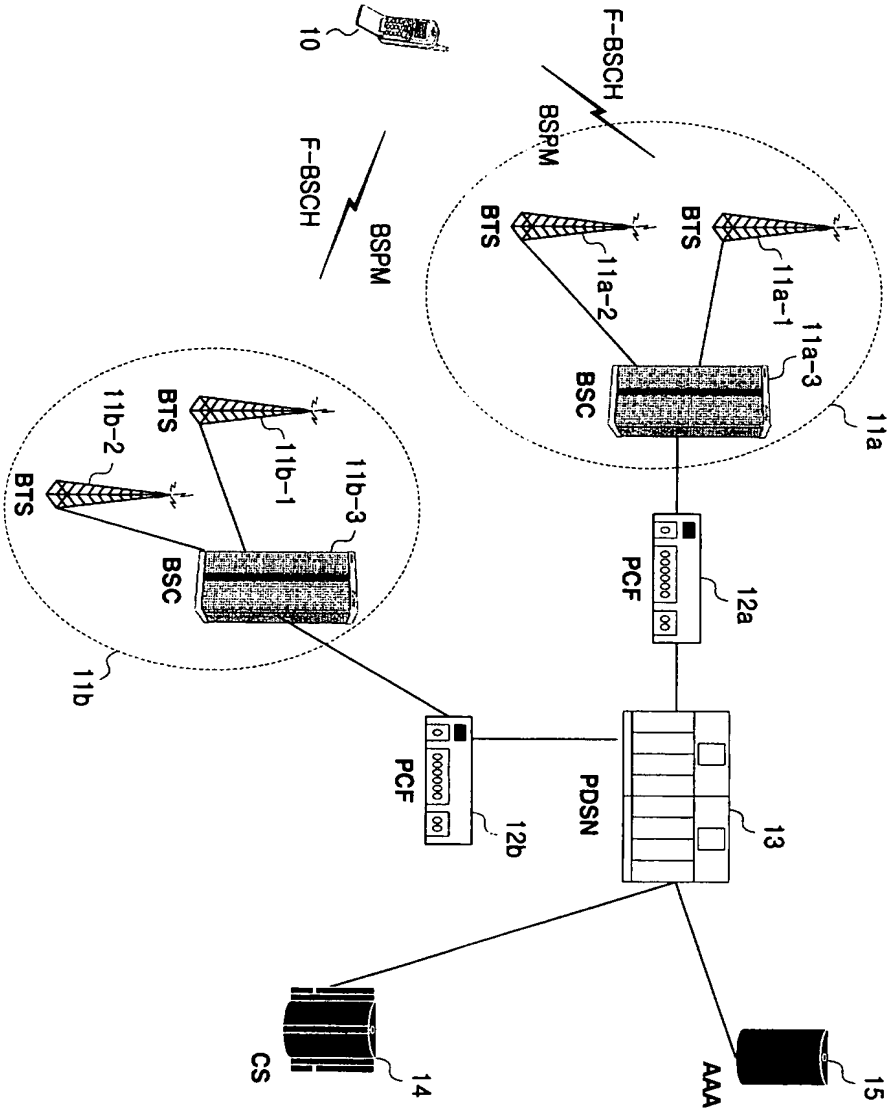
제 19 항에 있어서, 상기 암호화 정보 메시지는, 현재 유효한 암호화 키와 상기 현재 암호화 키의 유효시간을 더 포함하는 것을 특징으로 하는 상기 방법.

【청구항 21】

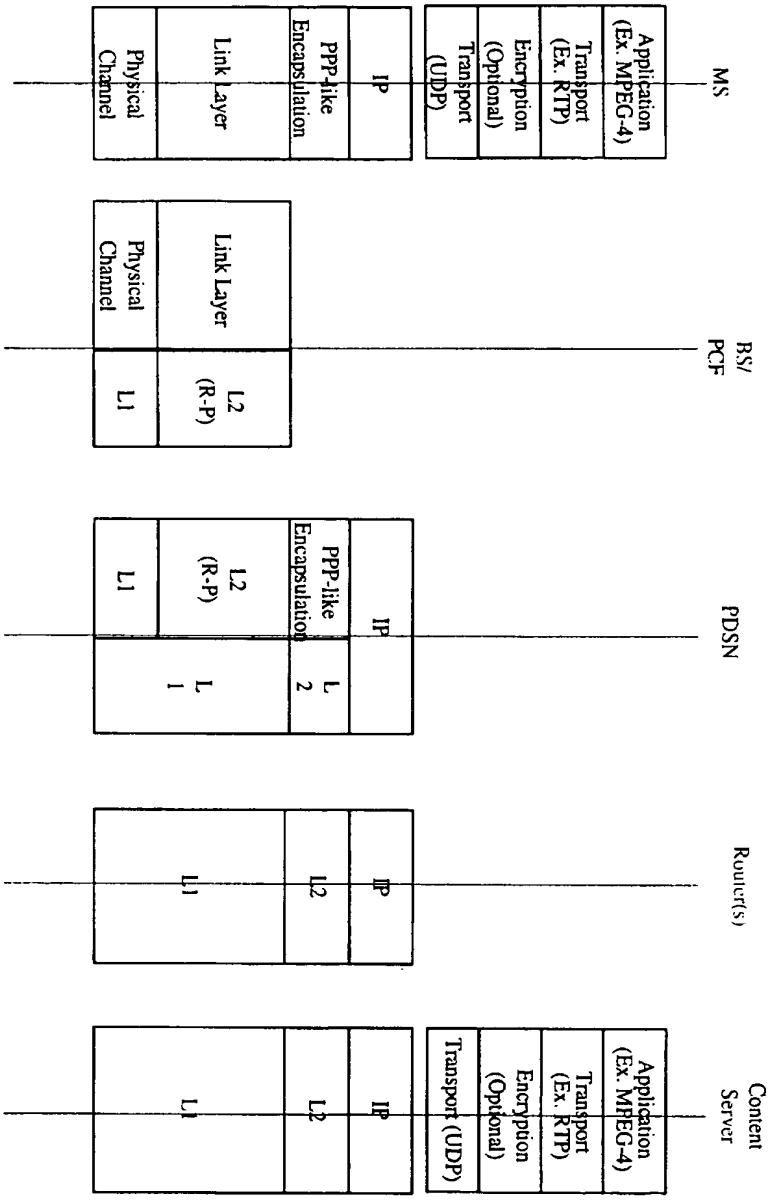
제 19 항에 있어서, 상기 유도시간은, 상기 기지국의 서비스영역 내에서 방송서비스중인 모든 단말들이 등록 메시지를 전송하는 주기들 중 최대의 주기보다 크도록 정해지는 것을 특징으로 하는 상기 방법.

【도면】

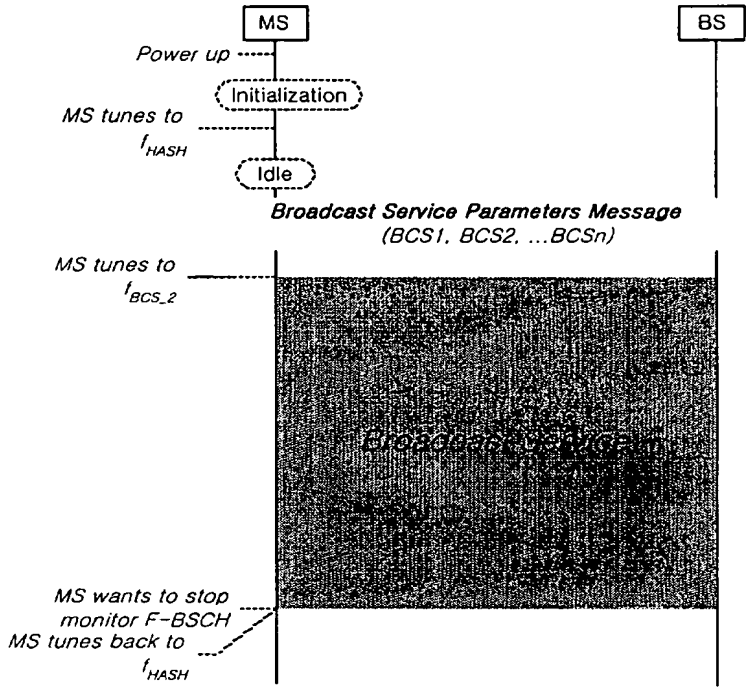
【도 1】


10
F-BSCH
BSRM
F-BSCH
BSPM
BTS
BTS
11a-2
11a-1
11a-3
BSC
11a
PCF
12a
BTS
BTS
11b-2
11b-1
11b-3
BSC
11b
PCF
12b
PDSN
13
CS
14
AAA
15

【도 2】


MS
BS/
PCF
PDSN
Router(s)
Content
Server
Application
(Ex. MPEG-4)
Transport
(Ex. RTP)
Encryption
(Optional)
Transport (UDP)
IP
PPP-like
Encapsulation
Link Layer
Physical
Channel
L2
(R-P)
L1
L2
L1

【도 3】


MS
BS
Power up
Initialization
MS tunes to
f_{HASH}
Idle
Broadcast Service Parameters Message
(BCS1, BCS2, ...BCSn)
MS tunes to
f_{BCS_2}
MS wants to stop
monitor F-BSCH
MS tunes back to
f_{HASH}

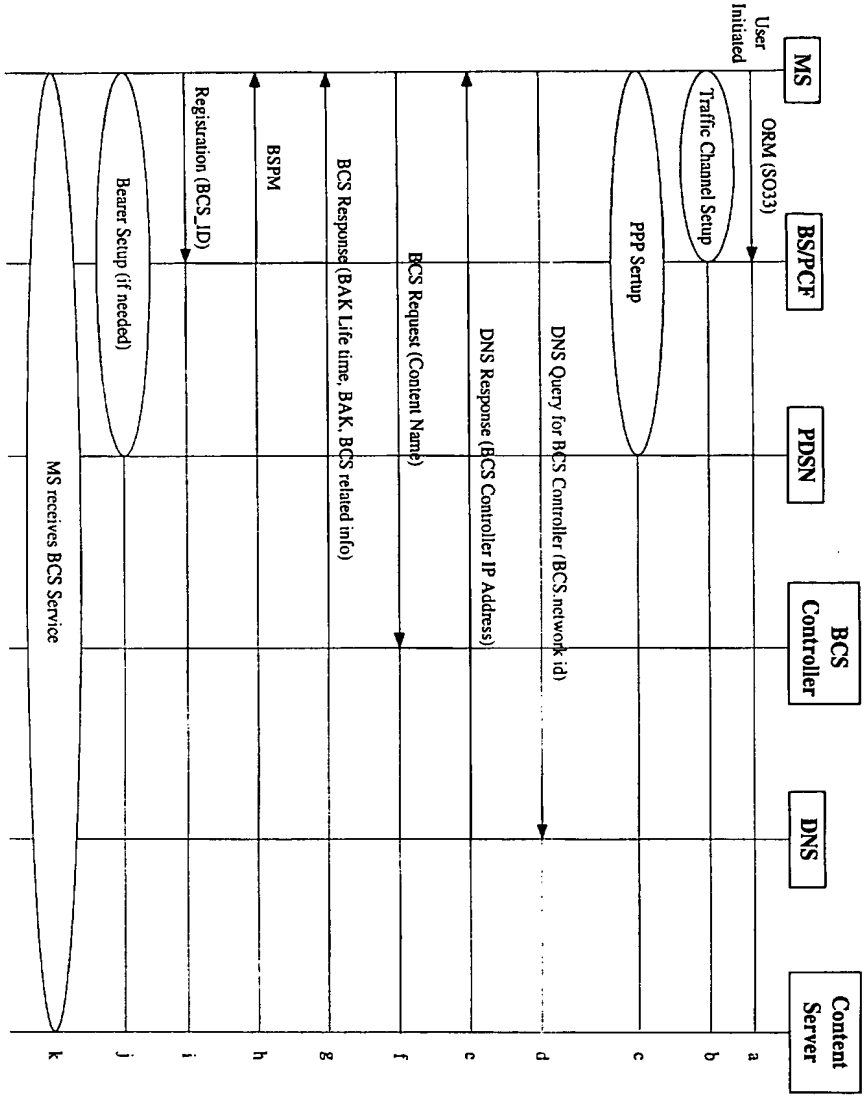
【도 4】

REGISTRATION MESSAGE

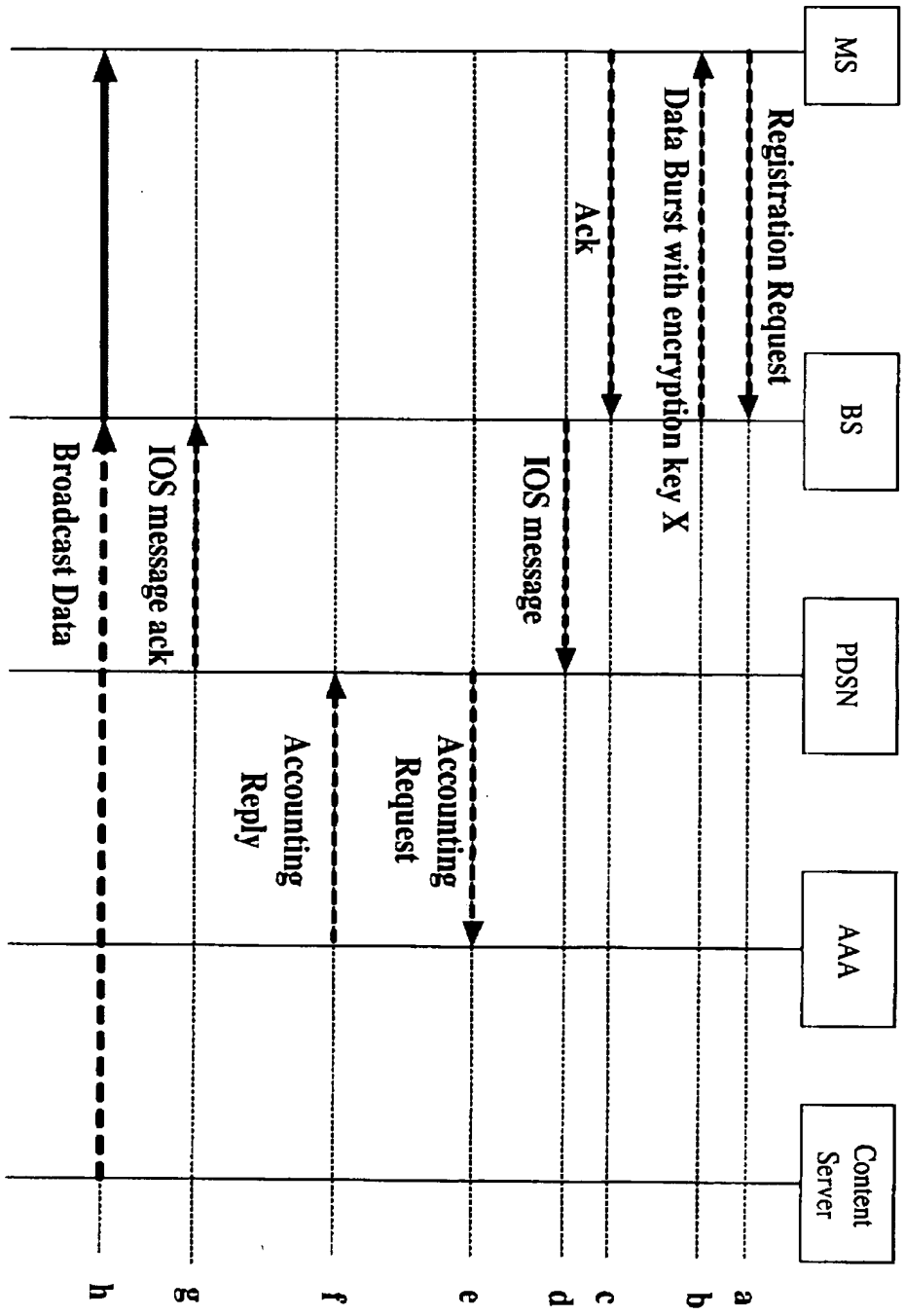
FIELD	**LENGTH (bits)**
REG_TYPE	4
...	
NUM_BCS_SESSION	0 or 6
NUM_BCS_SESSION occurrences of the following field	
BCS_ID	32
DE_REG_IND	1

REG_TYPE(binary)	Type of Registration
0000	Timer based
0001	Power up
0010	Zone based
0011	Power down
0100	Parameter change
0101	Ordered
0110	Distance based
0111	User Zone based
1000	BCS Session
...	reversed

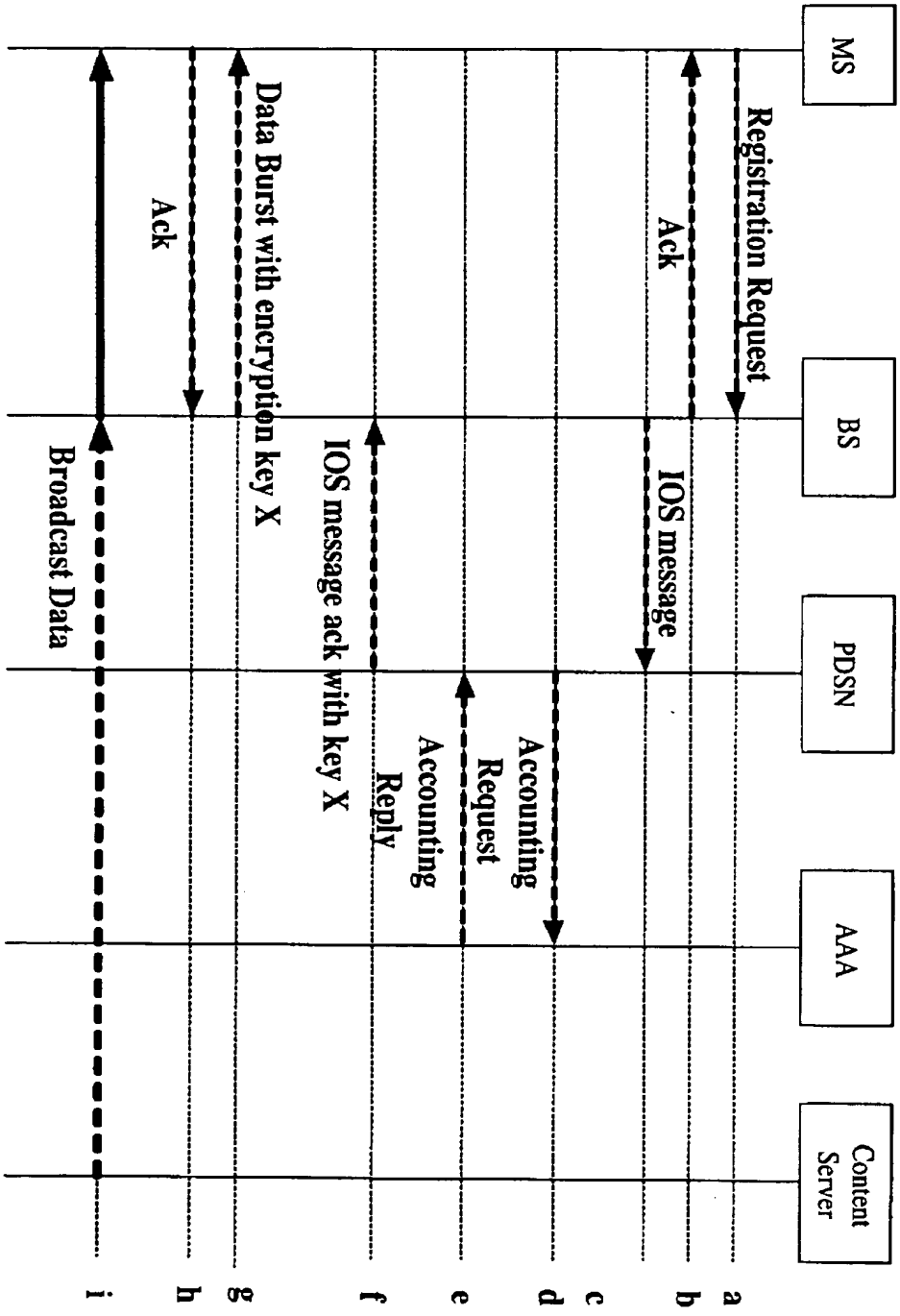
【도 5】


MS
BS/PCF
PDSN
BCS Controller
DNS
Content Server
User Initiated
ORM (SO33)
Traffic Channel Setup
PPP Setup
DNS Query for BCS Controller (BCS.network id)
DNS Response (BCS Controller IP Address)
BCS Request (Content Name)
BCS Response (BAK Life time, BAK, BCS related info)
BSPM
Registration (BCS_ID)
Bearer Setup (if needed)
MS receives BCS Service
a
b
c
d
e
f
g
h
i
j
k

【도 6】


MS
BS
PDSN
AAA
Content Server
Registration Request
Data Burst with encryption key X
Ack
IOS message
Accounting Request
Accounting Reply
IOS message ack
Broadcast Data
a
b
c
d
e
f
g
h

【도 7】

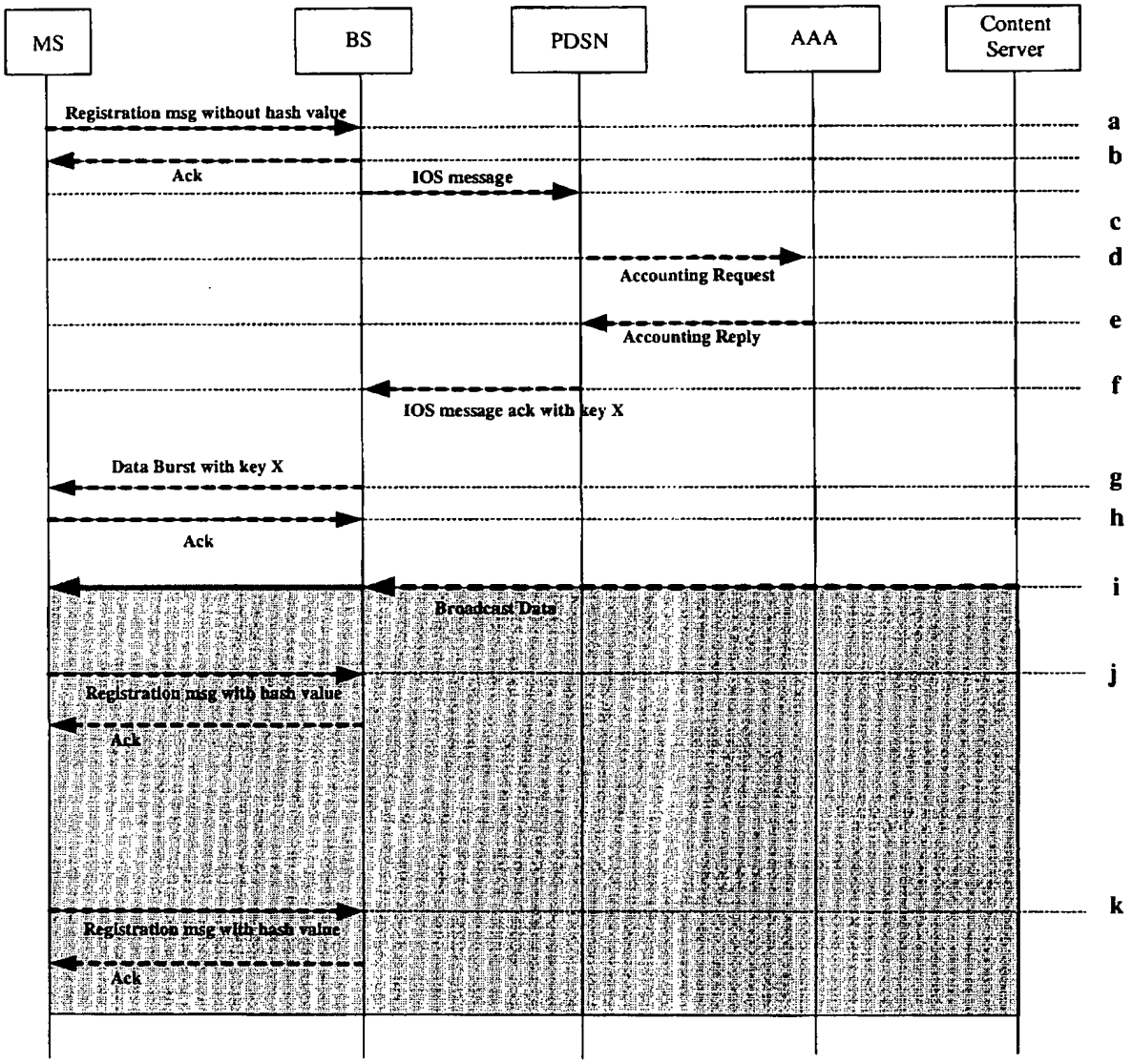

MS
BS
PDSN
AAA
Content Server
Registration Request
Ack
IOS message
Accounting Request
Accounting Reply
IOS message ack with key X
Data Burst with encryption key X
Ack
Broadcast Data
a
b
c
d
e
f
g
h
i

【도 8】

REGISTRATION MESSAGE

FIELD	**LENGTH (bits)**
REG_TYPE	4
...	
NUM_BCS_SESSION	0 or 6
NUM_BCS_SESSION occurrences of the following fields:	
BCS_ID	32
DE_REG_IND	1
ENCRYPTION_KEY_HASH_INCL	1
ENCRYPTION_KEY_HASH	0 or 4

【도 9】


MS
BS
PDSN
AAA
Content Server
Registration msg without hash value
a
Ack
b
IOS message
c
d
Accounting Request
Accounting Reply
e
f
IOS message ack with key X
Data Burst with key X
g
h
Ack
i
Broadcast Data
j
Registration msg with hash value
Ack
k
Registration msg with hash value
Ack

【도 10】

REGISTRATION MESSAGE

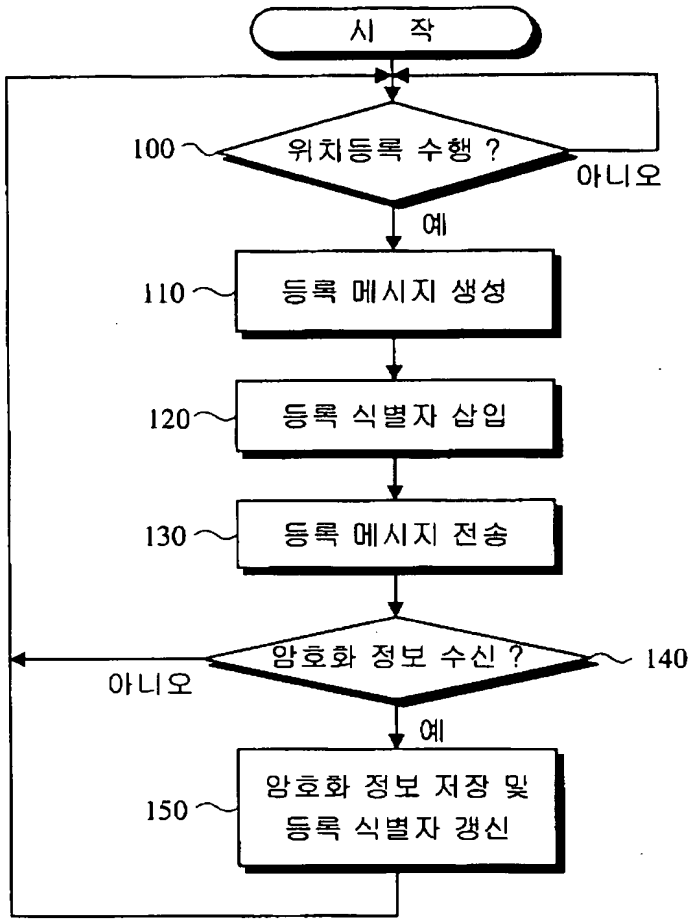
FIELD	**LENGTH (bits)**
REG_TYPE	4
...	
NUM_BCS_SESSION	0 or 6
NUM_BCS_SESSION occurrences of the following fields:	
BCS_ID	32
DE_REG_IND	1
ENCRYPTION_KEY_SEQ_INCL	1
ENCRYPTION_KEY_SEQ	0 or 2

【도 11】

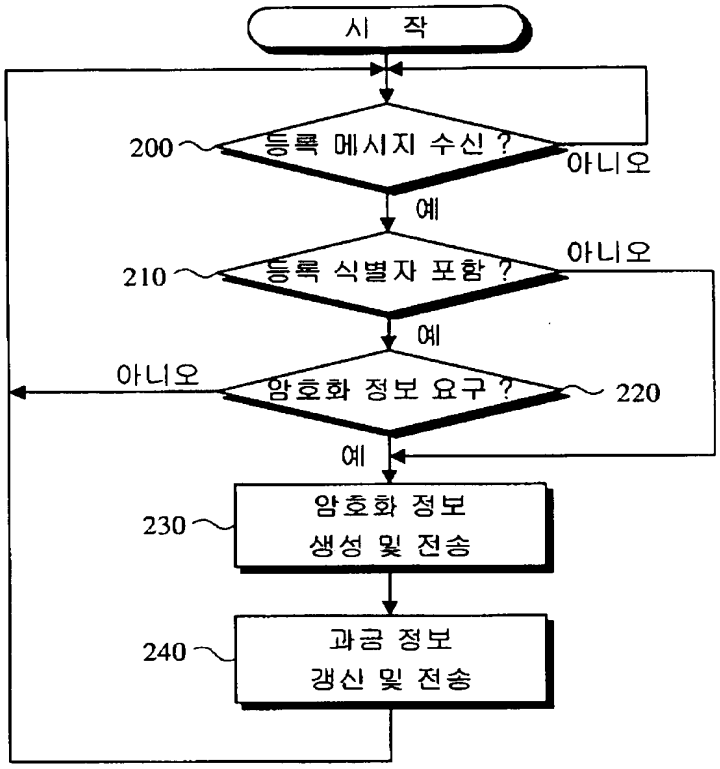
REGISTRATION MESSAGE

FIELD	**LENGTH (bits)**
REG_TYPE	4
...	
NUM_BCS_SESSION	0 or 6
NUM_BCS_SESSION occurrences of the following fields:	
BCS_ID	32
DE_REG_IND	1
ENCRYPTION_KEY_REQ	1

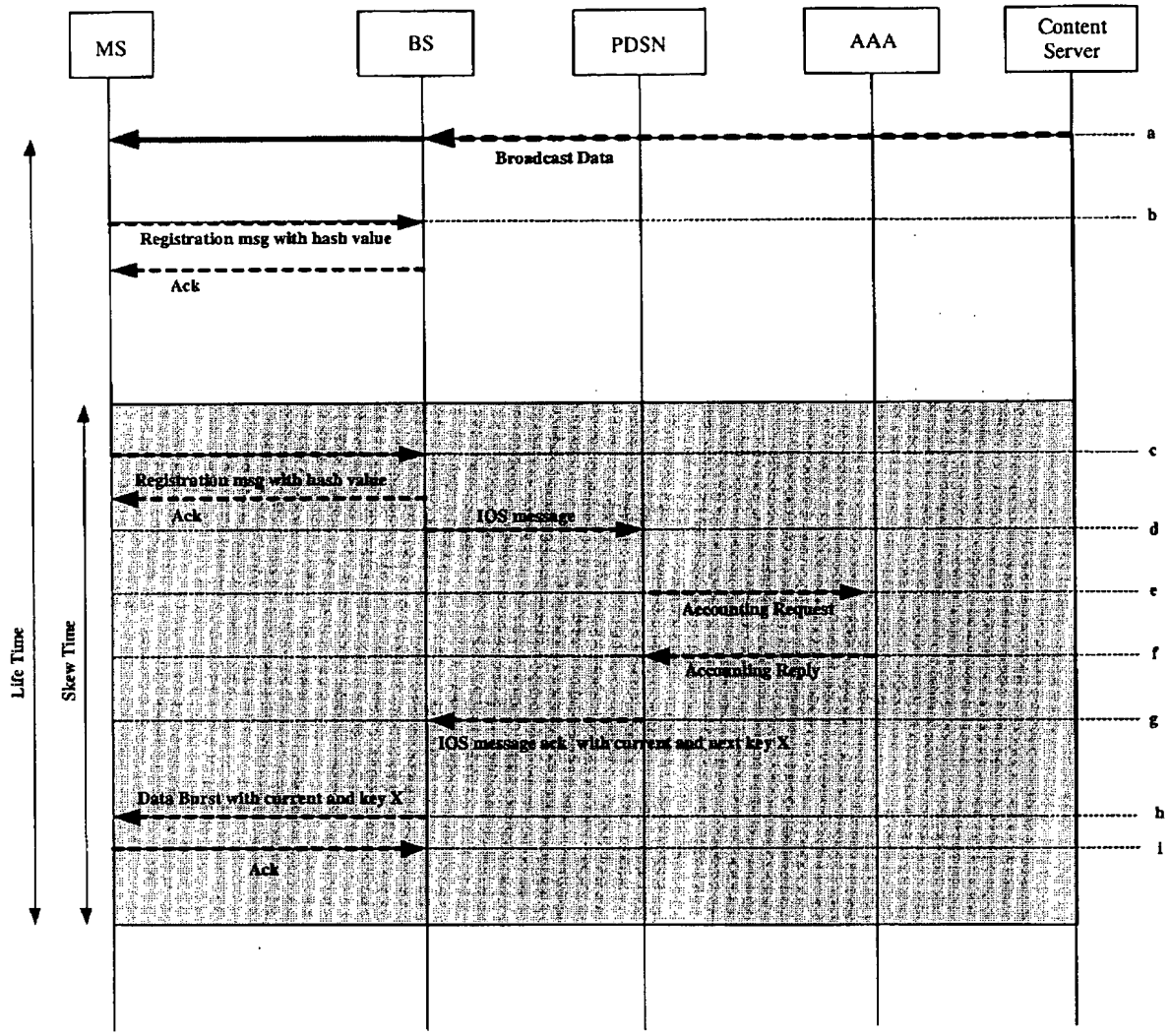
【도 12】


시 작
100
위치등록 수행 ?
아니오
예
110
등록 메시지 생성
120
등록 식별자 삽입
130
등록 메시지 전송
암호화 정보 수신 ?
140
아니오
예
150
암호화 정보 저장 및
등록 식별자 갱신

【도 13】


시 작
200
등록 메시지 수신 ?
아니오
예
210
등록 식별자 포함 ?
아니오
예
아니오
암호화 정보 요구 ?
220
예
230
암호화 정보
생성 및 전송
240
과금 정보
갱신 및 전송

【도 14】


MS
BS
PDSN
AAA
Content Server
Broadcast Data
Registration msg with hash value
Ack
Registration msg with hash value
Ack
IOS message
Accounting Request
Accounting Reply
IOS message ack. with current and next key X
Data Burst with current and key X
Ack
Life Time
Skew Time
a
b
c
d
e
f
g
h
i

【도 15】

DATA BURST MESSAGE (DBM)

FIELD	LENGTH (bits)
MSG_NUMBER	8
BURST_TYPE	6
NUM_MSGS	8
NUM_FIELDS	8
NUM_FIELDS occurences of the following fields:	
CHARi	8

CHARi

FIELD	LENGTH (bits)
NUM_BCS_SESSION	6
NUM_BCS_SESSION occurrences of the following fields:	
BCS_ID	32
ENCRYPTION_KEY	8
ENCRYPTION_KEY_LIFETIME	12
ENCRYPTION_KEY_SEQ_INCL	1
ENCRYPTION_KEY_SEQ	0 or 2
NEXT_ENCRYPTION_KEY_INCL	1
NEXT_ENCRYPTION_KEY	0 or 8
NEXT_ENCRYPTION_KEY_LIFETIME	0 or 12

【도 16】

ENCRYPTION INFORMATION MESSAGE (EIM)

FIELD	**LENGTH (bits)**
NUM_BCS_SESSION	6
NUM_BCS_SESSION occurrences of the following fields:	
BCS_ID	32
ENCRYPTION_KEY	8
ENCRYPTION_KEY_LIFETIME	12
ENCRYPTION_KEY_SEQ_INCL	1
ENCRYPTION_KEY_SEQ	0 or 2
NEXT_ENCRYPTION_KEY_INCL	1
NEXT_ENCRYPTION_KEY	0 or 8
NEXT_ENCRYPTION_KEY_LIFETIME	12